PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-313667
(43)Date of publication of application : 09.11.2001

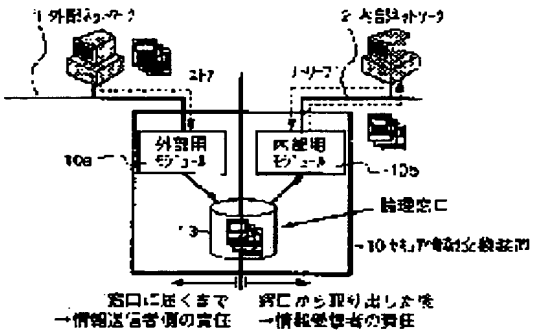
(51)Int.Cl. H04L 12/54
H04L 12/58
G09C 1/00
H04L 12/22

(21)Application number : 2000-130677
(22)Date of filing : 28.04.2000

(71)Applicant : RICOH CO LTD
NEW MEDIA DEVELOPMENT ASSOCIATION
(72)Inventor : KANAI YOICHI
YANAIDA MASUYOSHI

(54) SYSTEM AND METHOD FOR EXCHANGING SECURE INFORMATION AND COMPUTER READABLE RECORDING MEDIUM FOR RECORDING PROGRAM TO MAKE COMPUTER PERFORM THE METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To efficiently exchange information between networks while relieving the burden of manual labor and keeping independency in the networks.
SOLUTION: A system is provided with a secure information exchange device 10 for storing exchange data in a large capacity storage device 13 when an external module 10a receives exchange data from an external network 1, taking out exchange data corresponding to a takeout request from the device 13 when an internal module 10b receives the exchange data takeout request from an internal network 2 and outputting it.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２００１－３１３６６７
(P２００１－３１３６６７A)
(43)公開日　平成13年11月9日(2001.11.9)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
H04L	12/54		G09C	1/00	640 A	5J104
	12/58				660 E	5K030
G09C	1/00	640	H04L	11/20	101 B	9A001
		660		11/26		
H04L	12/22					

審査請求　未請求　請求項の数２４　ＯＬ　（全２９頁）

(21)出願番号　特願2000-130677(P2000-130677)

(22)出願日　平成12年4月28日(2000.4.28)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込1丁目3番6号

(71)出願人　596062738
財団法人ニューメディア開発協会
東京都港区三田1－4－28

(72)発明者　金井　洋一
東京都大田区中馬込1丁目3番6号　株式会社リコー内

(74)代理人　100104190
弁理士　酒井　昭徳

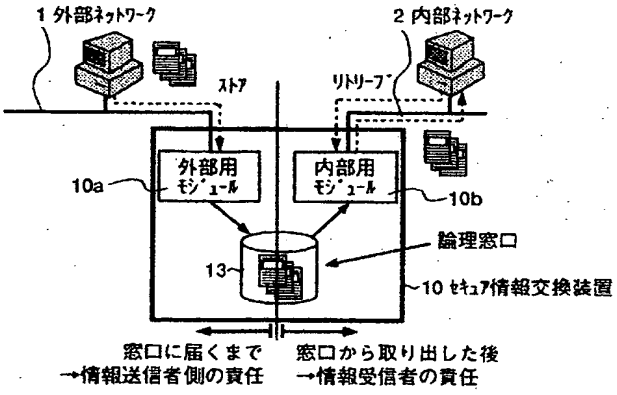
最終頁に続く

(54)【発明の名称】セキュア情報交換システム、セキュア情報交換方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】

【課題】　人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうこと

【解決手段】　外部用モジュール１０ａが外部ネットワーク１から交換データを受け付けた際に、該交換データを大容量記憶装置１３に格納し、内部用モジュール１０ｂが内部ネットワーク２から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを大容量記憶装置１３から取り出して出力するセキュア情報交換装置１０を設ける。



1

【特許請求の範囲】

【請求項１】　第１のネットワーク上に位置する第１の端末装置と第２のネットワーク上に位置する第２の端末装置との間で情報交換をおこなうセキュア情報交換システムにおいて、

前記第１の端末装置または第２の端末装置から受け付けた交換データを一時記憶する記憶手段と、

前記第１の端末装置から交換データを受け付けた際に、該交換データを前記記憶手段に格納する第１のモジュールと、

前記第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを前記記憶手段から取り出して当該第２の端末装置に出力する第２のモジュールと、

からなるセキュア情報交換装置を前記第１のネットワークおよび第２のネットワークの間に配設したことを特徴とするセキュア情報交換システム。

【請求項２】　前記第１のモジュールは、

前記第１の端末装置から交換データを受け付ける受付手段と、

前記受付手段により受け付けられた交換データについての第１の改ざん検知コードを算定する第１の算定手段と、

前記第１の算定手段により算定された第１の改ざん検知コードを当該交換データと対応づけて前記記憶手段に格納する第１の格納手段と、

を備え、

前記第２のモジュールは、

前記第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第１の改ざん検知コードを前記記憶手段から取り出す取出手段と、

前記取出手段により取り出された第１の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証する第１の検証手段と、

を備えたことを特徴とする請求項１に記載のセキュア情報交換システム。

【請求項３】　前記第１のモジュールは、複数の交換データを含むリストについての第２の改ざん検知コードを算定する第２の算定手段と、前記第２の算定手段により算定された第２の改ざん検知コードを前記リストとともに前記記憶手段に格納する第２の格納手段と、

を備え、

前記第２のモジュールは、前記第２の改ざん検知コードに基づいて前記リストの改ざんの有無を検証する第２の検証手段をさらに備えたことを特徴とする請求項２に記載のセキュア情報交換システム。

【請求項４】　前記第１のモジュールおよび第２のモジュールは、前記記憶手段に記憶した交換データの編集要求並びに削除要求を拒否する拒否手段をさらに備えたことを特徴とする請求項１、２または３に記載のセキュア情報交換システム。

2

【請求項５】　前記第１のモジュールは、

前記第１の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成する作成手段と、

前記受取証作成手段により作成された受取証データを前記第１の端末装置に返送する返送手段と、

をさらに備えたことを特徴とする請求項１～４のいずれか一つに記載のセキュア情報交換システム。

【請求項６】　前記作成手段は、前記交換データの特徴量を含む受取証データを作成することを特徴とする請求項５に記載のセキュア情報交換システム。

【請求項７】　前記作成手段は、前記交換データを特定する識別情報を含む受取証データを作成することを特徴とする請求項５または６に記載のセキュア情報交換システム。

【請求項８】　前記作成手段は、前記受取証データの受取内容についての第３の改ざん検知コードを生成し、該生成した第３の改ざん検知コードを含む受取証データを作成することを特徴とする請求項５、６または７に記載のセキュア情報交換システム。

【請求項９】　前記第１のモジュールは、

前記第１の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが前記第２の端末装置に送出済みであるか否かを確認する送出確認手段と、

前記送出確認手段による確認結果を前記第１の端末装置に通知する送出確認通知手段と、

をさらに備えたことを特徴とする請求項５～８のいずれか一つに記載のセキュア情報交換システム。

【請求項１０】　前記第１のモジュールは、

前記第１の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが前記記憶手段に記憶されているか否かを確認する記憶確認手段と、

前記記憶確認手段により前記記憶手段に当該交換データが記憶されていることを確認された際に、当該交換データを前記記憶手段から削除する削除手段と、

前記交換データの削除の有無を前記第１の端末装置に通知する削除通知手段と、

をさらに備えたことを特徴とする請求項５～９のいずれか一つに記載のセキュア情報交換システム。

【請求項１１】　前記第１の改ざん検知コード、第２の改ざん検知コードまたは第３の検知コードは、装置内部に保持した秘密鍵を用いて算定した電子署名であることを特徴とする請求項１～１０のいずれか一つに記載のセキュア情報交換システム。

【請求項１２】　前記第１のモジュールおよび第２のモジュールは、耐タンパー性を有する筐体に格納されたこ

とを特徴とする請求項１～１１のいずれか一つに記載のセキュア情報交換システム。

【請求項１３】　第１のネットワーク上に位置する第１の端末装置と第２のネットワーク上に位置する第２の端末装置との間で情報交換をおこなうセキュア情報交換方法において、

前記第１の端末装置から交換データを受け付けた際に、該交換データを所定の記憶部に格納する格納工程と、

前記第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを前記記憶部から取り出して当該第２の端末装置に出力する出力工程と、

を含んだことを特徴とするセキュア情報交換方法。

【請求項１４】　前記格納工程は、

前記第１の端末装置から交換データを受け付ける受付工程と、

前記受付工程により受け付けられた交換データについての第１の改ざん検知コードを算定する第１の算定工程と、

前記第１の算定工程により算定された第１の改ざん検知コードを当該交換データと対応づけて前記記憶部に格納する第１の格納工程と、

を含み、

前記出力工程は、

前記第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第１の改ざん検知コードを前記記憶部から取り出す取出工程と、

前記取出工程により取り出された第１の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証する第１の検証工程と、

を含んだことを特徴とする請求項１３に記載のセキュア情報交換方法。

【請求項１５】　前記格納工程は、

複数の交換データを含むリストについての第２の改ざん検知コードを算定する第２の算定工程と、

前記第２の算定工程により算定された第２の改ざん検知コードを前記リストとともに前記記憶部に格納する第２の格納工程と、

を含み、

前記出力工程は、前記第２の改ざん検知コードに基づいて前記リストの改ざんの有無を検証する第２の検証工程をさらに含んだことを特徴とする請求項１４に記載のセキュア情報交換方法。

【請求項１６】　前記記憶部に記憶した交換データの編集要求並びに削除要求を拒否する拒否工程をさらに含んだことを特徴とする請求項１３、１４または１５に記載のセキュア情報交換方法。

【請求項１７】　前記格納工程は、

前記第１の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成する作成工程と、

前記受取証作成工程により作成された受取証データを前記第１の端末装置に返送する返送工程と、

をさらに含んだことを特徴とする請求項１３～１６のいずれか一つに記載のセキュア情報交換方法。

【請求項１８】　前記作成工程は、前記交換データの特徴量を含む受取証データを作成することを特徴とする請求項１７に記載のセキュア情報交換方法。

【請求項１９】　前記作成工程は、前記交換データを特定する識別情報を含む受取証データを作成することを特徴とする請求項１７または１８に記載のセキュア情報交換方法。

【請求項２０】　前記作成工程は、前記受取証データの受取内容についての第３の改ざん検知コードを生成し、該生成した第３の改ざん検知コードを含む受取証データを作成することを特徴とする請求項１７、１８または１９に記載のセキュア情報交換方法。

【請求項２１】　前記格納工程は、

前記第１の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが前記第２の端末装置に送出済みであるか否かを確認する送出確認工程と、

前記送出確認工程による確認結果を前記第１の端末装置に通知する送出確認通知工程と、

をさらに含んだことを特徴とする請求項１７～２０のいずれか一つに記載のセキュア情報交換方法。

【請求項２２】　前記格納工程は、

前記第１の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが前記記憶部に記憶されているか否かを確認する記憶確認工程と、

前記記憶確認工程により前記記憶部に当該交換データが記憶されていることを確認された際に、当該交換データを前記記憶部から削除する削除工程と、

前記交換データの削除の有無を前記第１の端末装置に通知する削除通知工程と、

をさらに含んだことを特徴とする請求項１７～２１のいずれか一つに記載のセキュア情報交換方法。

【請求項２３】　前記第１の改ざん検知コード、第２の改ざん検知コードまたは第３の検知コードは、装置内部に保持した秘密鍵を用いて算定した電子署名であることを特徴とする請求項１３～２２のいずれか一つに記載のセキュア情報交換方法。

【請求項２４】　前記請求項１３～２３に記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、第１のネットワ

ーク上に位置する第１の端末装置と第２のネットワーク上に位置する第２の端末装置との間で情報交換をおこなうセキュア情報交換システム、セキュア情報交換方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体に関し、特に、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうことができるセキュア情報交換システム、セキュア情報交換方法、および方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【０００２】

【従来の技術】現在のネットワークシステムでは、ルータやゲートウエイなどを介してネットワークを互いに接続してネットワーク間の情報伝達がなされることが多い。このため、広域にわたって情報伝達が可能となる反面、プライバシー保護、情報漏洩および不正アクセスなどが問題となる。

【０００３】したがって、ネットワーク上に企業や公的機関の根幹をなす重要なデータが存在する場合には、このネットワークをインターネットなどの他のネットワークシステムと接続することが好ましくない。たとえば、人事データベースなどがある企業の基幹系ネットワークは、一般の事務系ネットワークと接続するのは好ましくないし、地方自治体における住民データが存在する基幹系ネットワークについても事務系ネットワークと接続するのは好ましくない。

【０００４】しかしながら、事務系ネットワーク上でおこなった業務処理結果を基幹系ネットワークに反映したり、事務系ネットワーク側の業務処理の中で基幹系ネットワーク上のデータを使用することができれば、業務効率が改善するのもまた事実である。

【０００５】このため、従来は、かかる場合に一方のネットワークでフロッピー（登録商標）ディスクなどのオフラインメディアにデータを保存し、他方のネットワークでそのデータを読み出すことにより、双方のネットワークの独立性を担保しつつ情報交換を可能にしている。

【０００６】ところが、かかる人手を介した情報交換をおこなっていたのでは、データ取得に時間を要し、また情報交換にかかる人的負担も大きいため、最近では、ファイアウオールを介してネットワークを接続し、許可されたプロトコルのみを中継または通過させるようにしてセキュリティを保持したまま情報交換をおこなうことが多い。

【０００７】このファイアウオールは、パケットの通過／遮断をおこなうパケットフィルタリングサービスと、社内クライアントのインターネットアクセスなどを代行するプロキシ（Ｐｒｏｘｙ）サービスとに大別され、ＯＳＩ（Ｏｐｅｎ　Ｓｙｓｔｅｍｓ　Ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ）参照モデルのネットワーク層やアプリケーション層などで機能するものが知られている。

【０００８】

【発明が解決しようとする課題】しかしながら、かかるファイアウオールによれば、不正なプロトコルを用いて一方のネットワークから他方のネットワークへ入ることはできないが、正しいプロトコルさえ用いれば他方のネットワークに進入可能な仕組み（ストア・フォワード型）となるので、双方のネットワークの独立性を保つことができなくなるという問題があった。

【０００９】図２３は、従来の典型的なファイアウオールの概念を説明するための説明図であり、同図に示す内部ネットワークは、外部ネットワークから直接的に作用される受動的なものとなるので、ネットワークの独立性を保つことができなくなるのである。

【００１０】また、外部ネットワークから内部ネットワークに情報交換用のデータを送信した場合に、どの時点でデータが受け渡しされたとするかが明確でないので、情報交換の途中でデータが改ざんまたは紛失すると、送信者側が悪いのか受信者側が悪いのか、どちらのネットワークに責任があるのかが不明確になるという問題もあった。

【００１１】これらのことから、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換をいかに効率よくおこなうかが極めて重要な課題となっている。

【００１２】この発明は、上述した従来技術による問題点を解決するためになされたものであり、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうことができるセキュア情報交換システム、セキュア情報交換方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【００１３】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、請求項１に記載の発明にかかるセキュア情報交換システムは、第１のネットワーク上に位置する第１の端末装置と第２のネットワーク上に位置する第２の端末装置との間で情報交換をおこなうセキュア情報交換システムにおいて、前記第１の端末装置または第２の端末装置から受け付けた交換データを一時記憶する記憶手段と、前記第１の端末装置から交換データを受け付けた際に、該交換データを前記記憶手段に格納する第１のモジュールと、前記第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを前記記憶手段から取り出して当該第２の端末装置に出力する第２のモジュールと、からなるセキュア情報交換装置を前記第１のネットワークおよび第２のネットワークの間に配設したことを特徴とする。

【００１４】この請求項１に記載の発明によれば、第１の端末装置から交換データを受け付けた際に、該交換データを記憶手段に格納し、第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを記憶手段から取り出して当該第２の端末装置に出力するセキュア情報交換装置を第１のネットワークおよび第２のネットワークの間に配設することとしたので、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうことができる。

【００１５】また、請求項２に記載の発明にかかるセキュア情報交換システムは、請求項１に記載の発明において、前記第１のモジュールが、前記第１の端末装置から交換データを受け付ける受付手段と、前記受付手段により受け付けられた交換データについての第１の改ざん検知コードを算定する第１の算定手段と、前記第１の算定手段により算定された第１の改ざん検知コードを当該交換データと対応づけて前記記憶手段に格納する第１の格納手段と、を備え、前記第２のモジュールが、前記第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第１の改ざん検知コードを前記記憶手段から取り出す取出手段と、前記取出手段により取り出された第１の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証する第１の検証手段と、を備えたことを特徴とする。

【００１６】この請求項２に記載の発明によれば、第１のモジュールでは、第１の端末装置から交換データを受け付け、受け付けた交換データについての第１の改ざん検知コードを算定し、算定した第１の改ざん検知コードを当該交換データと対応づけて記憶手段に格納し、第２のモジュールでは、第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第１の改ざん検知コードを記憶手段から取り出し、取り出した第１の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証することとしたので、交換データの改ざんを防止することができる。

【００１７】また、請求項３に記載の発明にかかるセキュア情報交換システムは、請求項２に記載の発明において、前記第１のモジュールが、複数の交換データを含むリストについての第２の改ざん検知コードを算定する第２の算定手段と、前記第２の算定手段により算定された第２の改ざん検知コードを前記リストとともに前記記憶手段に格納する第２の格納手段と、を備え、前記第２のモジュールが、前記第２の改ざん検知コードに基づいて前記リストの改ざんの有無を検証する第２の検証手段をさらに備えたことを特徴とする。

【００１８】この請求項３に記載の発明によれば、第１のモジュールでは、複数の交換データを含むリストについての第２の改ざん検知コードを算定し、算定した第２の改ざん検知コードをリストとともに記憶手段に格納し、第２のモジュールでは、第２の改ざん検知コードに基づいてリストの改ざんの有無を検証することとしたので、交換データをリスト構造で格納する場合にも、このリストの改ざんを効率よく防止することができる。

【００１９】また、請求項４に記載の発明にかかるセキュア情報交換システムは、請求項１～３に記載の発明において、前記第１のモジュールおよび第２のモジュールが、前記記憶手段に記憶した交換データの編集要求並びに削除要求を拒否する拒否手段をさらに備えたことを特徴とする。

【００２０】この請求項４に記載の発明によれば、第１のモジュールおよび第２のモジュールが、記憶手段に記憶した交換データの編集要求並びに削除要求を拒否することとしたので、交換データが編集や削除される被害を防止することができる。

【００２１】また、請求項５に記載の発明にかかるセキュア情報交換システムは、請求項１～４に記載の発明において、前記第１のモジュールが、前記第１の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成する作成手段と、前記受取証作成手段により作成された受取証データを前記第１の端末装置に返送する返送手段と、をさらに備えたことを特徴とする。

【００２２】この請求項５に記載の発明によれば、第１の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成し、作成した受取証データを第１の端末装置に返送することとしたので、交換データの受付を効率よく証明することができるとともに、該交換データの授受にかかる責任の所在を明らかにすることができる。

【００２３】また、請求項６に記載の発明にかかるセキュア情報交換システムは、請求項５に記載の発明において、前記作成手段が、前記交換データの特徴量を含む受取証データを作成することを特徴とする。

【００２４】この請求項６に記載の発明によれば、交換データの特徴量を含む受取証データを作成することとしたので、交換データと受取証の不整合を効率よく防止することができる。

【００２５】また、請求項７に記載の発明にかかるセキュア情報交換システムは、請求項５～６に記載の発明において、前記作成手段が、前記交換データを特定する識別情報を含む受取証データを作成することを特徴とする。

【００２６】この請求項７に記載の発明によれば、交換データを特定する識別情報を含む受取証データを作成することとしたので、該当する交換データを効率よく記憶手段から検索することができる。

【００２７】また、請求項８に記載の発明にかかるセキュア情報交換システムは、請求項５～７に記載の発明に

おいて、前記作成手段が、前記受取証データの受取内容についての第３の改ざん検知コードを生成し、該生成した第３の改ざん検知コードを含む受取証データを作成することを特徴とする。

【００２８】この請求項８に記載の発明によれば、受取証データの受取内容についての第３の改ざん検知コードを生成し、該生成した第３の改ざん検知コードを含む受取証データを作成することとしたので、この受取証データ自体の改ざんについても防止することができる。

【００２９】また、請求項９に記載の発明にかかるセキュア情報交換システムは、請求項５～８に記載の発明において、前記第１のモジュールが、前記第１の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが前記第２の端末装置に送出済みであるか否かを確認する送出確認手段と、前記送出確認手段による確認結果を前記第１の端末装置に通知する送出確認通知手段と、をさらに備えたことを特徴とする。

【００３０】この請求項９に記載の発明によれば、第１の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが第２の端末装置に送出済みであるか否かを確認し、この確認結果を第１の端末装置に通知することとしたので、送信確認を効率よくおこなうことができる。

【００３１】また、請求項１０に記載の発明にかかるセキュア情報交換システムは、請求項５～９に記載の発明において、前記第１のモジュールが、前記第１の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが前記記憶手段に記憶されているか否かを確認する記憶確認手段と、前記記憶確認手段により前記記憶手段に当該交換データが記憶されていることを確認された際に、当該交換データを前記記憶手段から削除する削除手段と、前記交換データの削除の有無を前記第１の端末装置に通知する削除通知手段と、をさらに備えたことを特徴とする。

【００３２】この請求項１０に記載の発明によれば、第１の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが記憶手段に記憶されているか否かを確認し、記憶手段に当該交換データが記憶されていることが確認された際に、当該交換データを記憶手段から削除し、交換データの削除の有無を第１の端末装置に通知することとしたので、誤って交換データを送信した場合であっても、該交換データの送信を効率よく取り消すことができる。

【００３３】また、請求項１１に記載の発明にかかるセキュア情報交換システムは、請求項１～１０に記載の発明において、前記第１の改ざん検知コード、第２の改ざん検知コードまたは第３の検知コードが、装置内部に保持した秘密鍵を用いて算定した電子署名であることを特徴とする。

【００３４】この請求項１１に記載の発明によれば、第１の改ざん検知コード、第２の改ざん検知コードまたは第３の検知コードを、装置内部に保持した秘密鍵を用いて算定した電子署名とすることとしたので、迅速かつ効率よく改ざんを防止することができる。

【００３５】また、請求項１２に記載の発明にかかるセキュア情報交換システムは、請求項１～１１に記載の発明において、前記第１のモジュールおよび第２のモジュールが、耐タンパー性を有する筐体に格納されたことを特徴とする。

【００３６】この請求項１２に記載の発明によれば、第１のモジュールおよび第２のモジュールを耐タンパー性を有する筐体に格納することとしたので、該第１のモジュールおよび第２のモジュール自体に対する不正な行為を防止することができる。

【００３７】また、請求項１３に記載の発明にかかるセキュア情報交換方法は、第１のネットワーク上に位置する第１の端末装置と第２のネットワーク上に位置する第２の端末装置との間で情報交換をおこなうセキュア情報交換方法において、前記第１の端末装置から交換データを受け付けた際に、該交換データを所定の記憶部に格納する格納工程と、前記第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを前記記憶部から取り出して当該第２の端末装置に出力する出力工程と、を含んだことを特徴とする。

【００３８】この請求項１３に記載の発明によれば、第１の端末装置から交換データを受け付けた際に、該交換データを記憶部に格納し、第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを記憶部から取り出して当該第２の端末装置に出力することとしたので、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうことができる。

【００３９】また、請求項１４に記載の発明にかかるセキュア情報交換方法は、請求項１３に記載の発明において、前記格納工程が、前記第１の端末装置から交換データを受け付ける受付工程と、前記受付工程により受け付けられた交換データについての第１の改ざん検知コードを算定する第１の算定工程と、前記第１の算定工程により算定された第１の改ざん検知コードを当該交換データと対応づけて前記記憶部に格納する第１の格納工程と、を含み、前記出力工程が、前記第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第１の改ざん検知コードを前記記憶部から取り出す取出工程と、前記取出工程により取り出された第１の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証する第１の検証工程と、を含んだことを特徴とする。

【００４０】この請求項１４に記載の発明によれば、第

１の端末装置から交換データを受け付け、受け付けた交換データについての第１の改ざん検知コードを算定し、算定した第１の改ざん検知コードを当該交換データと対応づけて記憶部に格納し、一方、第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第１の改ざん検知コードを記憶部から取り出し、取り出した第１の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証することとしたので、交換データの改ざんを防止することができる。

【００４１】また、請求項１５に記載の発明にかかるセキュア情報交換方法は、請求項１４に記載の発明において、前記格納工程が、複数の交換データを含むリストについての第２の改ざん検知コードを算定する第２の算定工程と、前記第２の算定工程により算定された第２の改ざん検知コードを前記リストとともに前記記憶部に格納する第２の格納工程と、を含み、前記出力工程が、前記第２の改ざん検知コードに基づいて前記リストの改ざんの有無を検証する第２の検証工程をさらに含んだことを特徴とする。

【００４２】この請求項１５に記載の発明によれば、複数の交換データを含むリストについての第２の改ざん検知コードを算定し、算定した第２の改ざん検知コードをリストとともに記憶部に格納し、第２のモジュールが、第２の改ざん検知コードに基づいてリストの改ざんの有無を検証することとしたので、交換データをリスト構造で格納する場合であっても、このリストの改ざんを効率よく防止することができる。

【００４３】また、請求項１６に記載の発明にかかるセキュア情報交換方法は、請求項１３～１５に記載の発明において、前記記憶部に記憶した交換データの編集要求並びに削除要求を拒否する拒否工程をさらに含んだことを特徴とする。

【００４４】この請求項１６に記載の発明によれば、記憶部に記憶した交換データの編集要求並びに削除要求を拒否できるとしたので、交換データが編集や削除される被害を防止することができる。

【００４５】また、請求項１７に記載の発明にかかるセキュア情報交換方法は、請求項１３～１６に記載の発明において、前記格納工程が、前記第１の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成する作成工程と、前記受取証作成工程により作成された受取証データを前記第１の端末装置に返送する返送工程と、をさらに含んだことを特徴とする。

【００４６】この請求項１７に記載の発明によれば、第１の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成し、作成した受取証データを第１の端末装置に返送することとしたので、交換データの受付を効率よく証明することができるとともに、該交換データの授受にかかる責任の所在を明らかにすることができる。

【００４７】また、請求項１８に記載の発明にかかるセキュア情報交換方法は、請求項１７に記載の発明において、前記作成工程が、前記交換データの特徴量を含む受取証データを作成することを特徴とする。

【００４８】この請求項１８に記載の発明によれば、交換データの特徴量を含む受取証データを作成することとしたので、交換データと受取証の不整合を効率よく防止することができる。

【００４９】また、請求項１９に記載の発明にかかるセキュア情報交換方法は、請求項１７～１８に記載の発明において、前記作成工程が、前記交換データを特定する識別情報を含む受取証データを作成することを特徴とする。

【００５０】この請求項１９に記載の発明によれば、交換データを特定する識別情報を含む受取証データを作成することとしたので、該当する交換データを効率よく記憶手段から検索することができる。

【００５１】また、請求項２０に記載の発明にかかるセキュア情報交換方法は、請求項１７～１９に記載の発明において、前記作成工程が、前記受取証データの受取内容についての第３の改ざん検知コードを生成し、該生成した第３の改ざん検知コードを含む受取証データを作成することを特徴とする。

【００５２】この請求項２０に記載の発明によれば、受取証データの受取内容についての第３の改ざん検知コードを生成し、該生成した第３の改ざん検知コードを含む受取証データを作成することとしたので、この受取証データ自体の改ざんについても防止することができる。

【００５３】また、請求項２１に記載の発明にかかるセキュア情報交換方法は、請求項１７～２０に記載の発明において、前記格納工程が、前記第１の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが前記第２の端末装置に送出済みであるか否かを確認する送出確認工程と、前記送出確認工程による確認結果を前記第１の端末装置に通知する送出確認通知工程と、をさらに含んだことを特徴とする。

【００５４】この請求項２１に記載の発明によれば、第１の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが第２の端末装置に送出済みであるか否かを確認し、この確認結果を第１の端末装置に通知することとしたので、送信確認を効率よくおこなうことができる。

【００５５】また、請求項２２に記載の発明にかかるセキュア情報交換方法は、請求項１７～２１に記載の発明において、前記格納工程が、前記第１の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが前記記憶部に記憶さ

れているか否かを確認する記憶確認工程と、前記記憶確認工程により前記記憶部に当該交換データが記憶されていることを確認された際に、当該交換データを前記記憶部から削除する削除工程と、前記交換データの削除の有無を前記第１の端末装置に通知する削除通知工程と、をさらに含んだことを特徴とする。

【００５６】この請求項２２に記載の発明によれば、第１の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが記憶部に記憶されているか否かを確認し、記憶部に当該交換データが記憶されていることが確認された際に、当該交換データを記憶部から削除し、交換データの削除の有無を第１の端末装置に通知することとしたので、誤って交換データを送信した場合であっても、該交換データの送信を効率よく取り消すことができる。

【００５７】また、請求項２３に記載の発明にかかるセキュア情報交換方法は、請求項１３～２２に記載の発明において、前記第１の改ざん検知コード、第２の改ざん検知コードまたは第３の検知コードが、装置内部に保持した秘密鍵を用いて算定した電子署名であることを特徴とする。

【００５８】この請求項２３に記載の発明によれば、第１の改ざん検知コード、第２の改ざん検知コードまたは第３の検知コードを、装置内部に保持した秘密鍵を用いて算定した電子署名とすることとしたので、迅速かつ効率よく改ざんを防止することができる。

【００５９】また、請求項２４に記載の発明にかかる記録媒体は、請求項１３～２３のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムを機械読み取り可能となり、これによって、請求項１３～２３のいずれか一つの動作をコンピュータによって実現することができる。

【００６０】

【発明の実施の形態】以下に添付図面を参照して、この発明にかかるセキュア情報交換システム、セキュア情報交換方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【００６１】（セキュア情報交換システムの概念）まず最初に、本実施の形態で用いるセキュア情報交換システムの概念について説明する。図１は、本実施の形態で用いるセキュア情報交換システムの概念を説明するための説明図である。

【００６２】図１示すように、このセキュア情報交換システムは、インターネットなどの外部ネットワーク１と内部ネットワーク２の間にセキュア情報交換装置１０を配設したシステム構成となり、このセキュア情報交換装置１０内部には、外部用モジュール１０ａ、内部用モジュール１０ｂおよび大容量記憶装置１３を有している。

【００６３】このセキュア情報交換装置１０は、外部ネットワーク１または内部ネットワーク２の一方から外部用モジュール１０ａまたは内部用モジュール１０ｂが交換データを受け取り、これを一時的に大容量記憶装置１３に保存する。そして、他方のネットワークから交換データの取り出しを要求されると、外部用モジュール１０ａまたは内部用モジュール１０ｂが保存した交換データを他方のネットワークに渡す。

【００６４】このように、かかるセキュア情報交換装置１０では、ストア・リトリーブ（Ｓｔｏｒｅ　ａｎｄ　Ｒｅｔｒｉｅｖｅ）方式を採用している。ここで、この大容量記憶装置１３は、論理窓口の役割を果たすことになる。なお、セキュア情報交換装置１０内部の大容量記憶装置１３に保存された交換データに不正なアクセスがおこなわれないように、このセキュア情報交換装置１０は交換データを保護する機能も有する。

【００６５】したがって、かかるセキュア交換システムを用いれば、異なるセキュリティポリシーを持つ２つのネットワークシステムの独立性を完全に保ったまま、双方のネットワークシステム間でオフラインメディアと人手を介さない情報交換が可能となる。

【００６６】また、このセキュア情報交換システムでは、セキュア情報交換装置１０に交換データを送り届けるまでが送信者側の責任であり、このセキュア情報交換装置１０から交換データを取り出した後は受信者側の責任とすることができるので、責任範囲が明確となる。

【００６７】図２は、図１に示したセキュア情報交換装置１０の配置位置の一例を示す図である。同図に示すように、住民基本台帳ネットワーク２０と、基幹ＬＡＮ２１と、情報系ＬＡＮ２２と、インターネット２３とをそれぞれ接続する場合には、住民基本台帳ネットワーク２０～基幹ＬＡＮ２１の間と、基幹ＬＡＮ２１～情報系ＬＡＮ２２の間と、情報系ＬＡＮ２２～インターネット２３の間とにそれぞれセキュア情報交換装置１０を配設することにより、各ネットワークの独立性を保持することになる。

【００６８】（セキュア情報交換装置の装置構成）つぎに、図１に示したセキュア情報交換装置１０の装置構成について具体的に説明する。図３は、図１に示したセキュア情報交換装置１０の装置構成を示すブロック図である。

【００６９】同図に示すように、外部モジュール１０ａが、外部ネットワーク１を介して該外部ネットワーク１上の端末装置１１によりアクセスされ、内部モジュール１０ｂが内部ネットワーク２を介して該内部ネットワーク２上の端末装置１２によりアクセスされる。そして、この外部モジュール１０ａおよび内部モジュール１０ｂは、物理的な耐タンパー性を有する筐体１００に格納され、それぞれ大容量記憶装置１３にデータを記憶することができる。

【００７０】外部モジュール１０ａは、通信ポート１１

０、一時記憶部１１１、内部記憶媒体１１２、プロセッサ１１３、内部タイマ１１４およびプログラム格納媒体１１５からなり、内部モジュール１０ｂは、通信ポート１２０、一時記憶部１２１、内部記憶媒体１２２、プロセッサ１２３、内部タイマ１２４およびプログラム格納媒体１２５からなる。

【００７１】通信ポート１１０または１２０は、外部システムまたは内部システムとの通信をするためのインターフェース部であり、たとえばイーサネット（登録商標）カードなどが該当する。ただし、外部ネットワーク１と内部ネットワーク２とで通信プロトコルが異なる場合もある。特に、基幹系のネットワークはイーサネットであるとは限らない。

【００７２】一時記憶部１１１または１２１は、プロセッサ１１３または１２３が処理するデータを一時記憶するメモリであり、読み書き可能なＲＡＭが該当する。この一時記憶部１１１には、電源が断にされた際に消去されても良いデータが記憶される。

【００７３】内部記憶媒体１１２または１２２は、外部モジュール１０ａまたは内部モジュール１０ｂの内部管理データなどを記憶する二次記憶媒体であり、ハードディスク装置などが該当する。

【００７４】プロセッサ１１３または１２３は、プログラム格納媒体１１５または１２５からプログラムをロードして実行するＣＰＵであり、内部タイマ１１４または１２４は、現在時刻を計時してプロセッサ１１３または１２３に供給するタイマである。

【００７５】プログラム格納媒体１１５または１２５は、セキュア情報交換装置１０が提供する情報交換サービスのプログラムが格納された媒体であり、ＲＯＭやハードディスク装置が該当する。

【００７６】耐タンパー筐体１００は、セキュア情報交換装置１０のプログラムや内部管理データ、タイマなどを不正に改ざん、消去されないよう、これらを外部からの物理的な攻撃から保護するための物理的な筐体である。なお、この耐タンパー筐体１００を無理に開けられた際には、内部管理データを消去したり、システム管理者に通報するよう構成することができる。また、システム管理者には開けることができないが、保守要員であれば開けられる鍵をかけることもできる。

【００７７】大容量記憶装置１３は、このセキュア情報交換装置１０が接続する双方のネットワーク（外部ネットワーク１および内部ネットワーク２）から渡される交換データを格納する二次記憶装置であり、ハードディスク装置などが該当する。交換データ保護の観点からＲＡＩＤとすることもできる。

【００７８】なお、この大容量記憶装置１３は、大容量のデータ交換がおこなわれるような場合には耐タンパー筐体１００内に収まらない可能性が高いので、ここでは耐タンパー筐体１００の外部に配設することとしたが、耐タンパー筐体１００の内部に配設しても良い。

【００７９】（セキュア情報交換装置の機能および処理内容）つぎに、図１に示したセキュア情報交換装置１０の機能および処理内容について説明する。このセキュア情報交換装置１０は、（ａ）データ交換機能、（ｂ）交換データ保護機能を有する。

【００８０】ここで、（ａ）データ交換機能とは、一方のネットワークから交換データを受け取り、他方のネットワークからのデータ取り出し要求に対してその交換データを渡す機能である。なお、一方のネットワークから受け取った交換データを他方のネットワークに自動的に転送することはない。他方のネットワークからデータが取り出されるまで交換データを大容量記憶装置１３に保持する。

【００８１】（ｂ）交換データ保護機能とは、内部に保持されている交換データが不正に改ざんされないよう該交換データを安全に保護する機能であり、一方のネットワークから受け取った交換データは、他方のネットワークから取り出されるまで内部に保持される。

【００８２】また、このセキュア情報交換装置１０は、図１に示したセキュア情報交換装置１０の機能および処理内容に示すように（１）サービス受付処理、（２）ストア処理、（３）交換データ一覧処理、（４）リトリーブ処理および（５）送出確認処理をおこなう。このサービス受付処理とは、セキュア情報交換装置１０にアクセスするユーザから様々なサービス処理要求を受け付け、その要求内容に応じて処理を割り振るものである。

【００８３】ストア処理とは、セキュア情報交換装置１０に対して送信された交換データを受け取ってシステム内部にストアする処理であり、交換データ一覧処理とは、セキュア情報交換装置１０内部で保持している交換データの識別番号の一覧を取得する処理である。

【００８４】リトリーブ処理とは、セキュア情報交換装置１０に対して送られた取り出し要求に対して、システム内部に保持されている交換データを送出する処理であり、送出確認処理とは、セキュア情報交換装置１０に対して送信された交換データが、すでに他方のネットワークで取り出されたか否かを確認する処理である。

【００８５】このように、かかるセキュア情報交換装置１０は、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうための機能を有している。以下、これらの処理の処理手順について順次説明する。

【００８６】（１）サービス受付処理

つぎに、図１に示したセキュア情報交換装置１０がおこなうサービス受け付け処理手順について具体的に説明する。図５は、図１に示したセキュア情報交換装置１０がおこなうサービス受け付け処理手順を示すフローチャートである。

【００８７】同図に示すように、このセキュア情報交換

装置１０は、まず最初にユーザが認証されているか否かを確認し（ステップＳ５０１）、ユーザが認証されていない場合には（ステップＳ５０１否定）、サービス処理要求がユーザ認証処理要求であるか否かを調べる（ステップＳ５０２）。

【００８８】その結果、ユーザ認証処理要求である場合には（ステップＳ５０２肯定）、ユーザ認証処理をおこなった後に（ステップＳ５０３）処理を終了し、ユーザ認証処理要求でない場合には（ステップＳ５０２否定）、エラー処理をおこなった後に（ステップＳ５１２）処理を終了する。

【００８９】これに対して、ユーザが認証されている場合には（ステップＳ５０１肯定）、サービス処理要求がストア処理要求であるか否かを調べ（ステップＳ５０４）、ストア処理要求である場合には（ステップＳ５０４肯定）、ストア処理をおこなって（ステップＳ５０５）処理を終了する。

【００９０】また、サービス処理要求がストア処理要求ではない場合には（ステップＳ５０４否定）、該サービス処理要求が交換データ一覧処理要求であるか否かを調べ（ステップＳ５０６）、交換データ一覧処理要求である場合には（ステップＳ５０６肯定）、交換データ一覧処理をおこなった後に（ステップＳ５０７）処理を終了する。

【００９１】また、サービス処理要求が交換データ一覧処理要求ではない場合には（ステップＳ５０６否定）、このサービス処理要求がリトリーブ処理要求であるか否かを調べ（ステップＳ５０８）、リトリーブ処理要求である場合には（ステップＳ５０８肯定）、リトリーブ処理をおこなった後に（ステップＳ５０９）処理を終了する。

【００９２】また、サービス処理要求がリトリーブ処理要求ではない場合には（ステップＳ５０８否定）、このサービス処理要求が送出確認処理要求であるか否かを調べ（ステップＳ５１０）、送出確認処理要求である場合には（ステップＳ５１０肯定）、送出確認処理要求をおこなった後に（ステップＳ５１１）処理を終了する。なお、サービス処理要求が送出確認処理要求ではない場合には（ステップＳ５１０否定）、エラー処理をおこなった後に（ステップＳ５１２）、処理を終了する。

【００９３】つぎに、図５のステップＳ５０３に示したユーザ認証処理手順についてさらに詳細に説明する。図６は、図５のステップＳ５０３に示したユーザ認証処理手順を示すフローチャートである。なおここでは、簡単なパスワード認証をおこなう場合を示すこととし、アカウント管理データは図７に示すように外部ネットワーク１用、内部ネットワーク２用に別々に内部記憶媒体１１２および１２２に記憶されるものとする。

【００９４】図６に示すように、まず最初に、内部記憶媒体１１２または１２２に記憶されたアカウント管理データを参照し（ステップＳ６０１）、このアカウント管理データの中で受け取ったアカウント名に対応するアカウントエントリを検索する（ステップＳ６０２）。

【００９５】そして、アカウントエントリが存在しない場合には（ステップＳ６０３否定）、エラー処理をおこなった（ステップＳ６０７）後に、処理を終了する。一方、アカウントエントリが存在する場合には（ステップＳ６０３肯定）、受け取ったパスワードとアカウントエントリにあるパスワードを照合する（ステップＳ６０４）。

【００９６】その結果、パスワードが一致した場合には（ステップＳ６０５肯定）、ユーザ認証済みであることを一時記憶部１１１または１２１で記憶する（ステップＳ６０６）。一方、ステップＳ６０５において、パスワードが一致しない場合には（ステップＳ６０５否定）、エラー処理をおこなった（ステップＳ６０７）のちに、処理を終了する。

【００９７】（２）ストア処理

つぎに、図１に示したセキュア情報交換装置１０がおこなうストア処理手順について具体的に説明する。図８は、図１に示したセキュア情報交換装置１０がおこなうストア処理手順を示すフローチャートであり、図９は、かかるストア処理の概念を説明するための説明図である。

【００９８】図８に示すように、このセキュア情報交換装置１０は、まず最初にユーザのアカウント名、受け取った論理窓口番号、アクセス種別（ストア）を元に後述する窓口アクセス権検査処理をおこない（ステップＳ８０１）、アクセス権があるか否かを確認する（ステップＳ８０２）。

【００９９】その結果、アクセス権がない場合には（ステップＳ８０２否定）、エラー処理をおこなった後に（ステップＳ８１０）処理を終了する。一方、ステップＳ８０２において、アクセス権がある場合には（ステップＳ８０２肯定）、受け取った交換データに交換データ識別番号を割り当て（ステップＳ８０３）、受け取った交換データに対して電子署名を計算し（ステップＳ８０４）、論理窓口番号、交換データ識別番号、電子署名を元に交換データリスト追加処理をおこなう（ステップＳ８０５）。

【０１００】そして、交換データ更新処理が成功したか否かを確認し（ステップＳ８０６）、失敗に終わった場合には（ステップＳ８０６否定）、エラー処理をおこなった（ステップＳ８１０）後に、すべての処理を終了する。

【０１０１】これに対して、交換データ更新処理が成功した場合（ステップＳ８０６肯定）には、交換データを大容量記憶装置１３の論理窓口番号に対応するディレクトリに交換データ識別番号をファイル名として格納し（ステップＳ８０７）、交換データ識別番号と格納した

論理窓口番号、電子署名を元に受取証作成処理をおこない（ステップＳ８０８）、作成された受取証データを交換データ送信元のユーザに送る（ステップＳ８０９）。

【０１０２】たとえば、図９に示す外部用モジュール１０ａが、コンピュータ１１からストア要求、論理窓口番号および交換データを受け取ると、「２０００３２８－０００００３２７」という交換データ識別番号を付与するとともに、その電子署名を計算して、大容量記憶装置１３の該当する論理窓口に交換データリストファイルを格納して、受取証データをコンピュータ１１を使用する交換データ送信元のユーザに送信することになる。

【０１０３】図１０は、かかる交換データリストファイルの構造を示す図であり、同図に示すように、この交換データリストファイルは、交換データ識別番号および交換データ電子署名からなるＮ個の交換データエントリ＃１～＃Ｎと、交換データリストに対する電子署名とからなる。

【０１０４】図１１は、受取証データの構造を示す図である。この図１１からもわかるように、かかる受取証データは、交換データ識別番号、格納した論理窓口番号および交換データ電子署名からなる受取内容と、その受取内容に対する電子署名とからなる。

【０１０５】なお、ここではコンピュータ１１とセキュア情報交換装置１０との間でのネットワークセキュリティについての説明を省略したが、ＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔｓ Ｌａｙｅｒ）などの既存の安全な通信プロトコルを使用することもできる。

【０１０６】また、ここでは受け取った交換データの内容についての説明を省略したが、交換データの内容についてコンテンツフィルタリングを実行することもできる。これにより、たとえば基幹系ネットワークから情報漏洩などが起こらないようにすることができる。

【０１０７】つぎに、図８のステップＳ８０１に示した窓口アクセス権検査処理手順について説明する。図１２は、図８のステップＳ８０１に示した窓口アクセス権検査処理手順を示すフローチャートであり、図１３は、論理窓口管理データの構造を示す図である。

【０１０８】図１２に示すように、この窓口アクセス権検査処理では、論理窓口データを内部記憶媒体から読み出し（ステップＳ１２０１）、受け取った論理窓口番号に対応する論理窓口管理データの管理エントリを参照して（ステップＳ１２０２）、管理エントリの内容がアカウント名、アクセス種別に適合しているか否かを調べる（ステップＳ１２０３）。

【０１０９】そして、管理エントリの内容がアカウント名、アクセス種別に適合していない場合には（ステップＳ１２０３否定）、エラー処理をおこなった後に（ステップＳ１２０４）処理を終了する。

【０１１０】この処理は、ユーザのアカウント名と論理窓口番号、アクセス種別（ストア、リトリーブ、一覧）

を受け取って処理する。論理窓口ごとに設定されているデータ交換方向とアクセス種別がマッチしなければアクセスを拒否することになる。なお、データ交換方向とは、一方のネットワークから他方のネットワークへデータを交換する方向のことを意味し、どちらの方向にデータ交換をおこなえるかが論理窓口ごとにあらかじめ設定されている。

【０１１１】かかる論理窓口管理データは、図１３に示すようにＮ個のアクセス許可エントリ＃１～＃Ｎからなるアクセス許可リスト、論理窓口番号、データ交換方向からなる複数の管理エントリを有する。

【０１１２】つぎに、図８のステップＳ８０５に示した交換データリスト追加処理手順について説明する。図１４は、図８のステップＳ８０５に示した交換データリスト追加処理手順を示すフローチャートである。

【０１１３】同図に示すように、この交換データリスト追加処理では、大容量記憶装置１３から論理窓口番号に対応する交換データリストファイルを読み出し（ステップＳ１４０１）、その後、交換データリスト検証処理をおこなう（ステップＳ１４０２）。

【０１１４】そして、検証に失敗した場合（ステップＳ１４０３否定）には、エラー処理をおこなった（ステップＳ１４０８）後に、処理を終了する。これに対して、検証に成功した場合には（ステップＳ１４０３肯定）、受け取った交換データ識別番号と電子署名で新しい交換データエントリを作成し（ステップＳ１４０４）する。

【０１１５】その後、作成した交換データエントリを交換データリストに追加し（ステップＳ１４０５）、交換データリスト署名処理をおこなった後に（ステップＳ１４０６）、大容量記憶装置１３に交換データリストファイルを格納する（ステップＳ１４０７）。

【０１１６】つぎに、図１４のステップＳ１４０２に示した交換データリスト検証処理手順について説明する。図１５は、図１４のステップＳ１４０２に示した交換データリスト検証処理手順を示すフローチャートである。

【０１１７】同図に示すように、この交換データリスト検証処理は、交換データリストファイルの正当性を検証するものであり、具体的には、交換データリストファイルに格納されている電子署名を参照し（ステップＳ１５０１）、交換データリストファイルに格納されている交換データリストに対してハッシュ値を計算し（ステップＳ１５０２）、内部記憶媒体に格納されている公開鍵で電子署名を復号して検証用ハッシュ値を得る（ステップＳ１５０３）。

【０１１８】その後、ハッシュ値と検証用ハッシュ値が一致するか否かを確認し（ステップＳ１５０４）、一致しない場合には（ステップＳ１５０４否定）、エラー処理をおこなった後に（ステップＳ１５０５）処理を終了する。

【０１１９】つぎに、図１４のステップＳ１４０６に示

した交換データリスト署名処理手順について説明する。図１６は、図１４のステップＳ１４０６に示した交換データリスト署名処理手順を示すフローチャートである。

【０１２０】同図に示すように、この交換データリスト署名処理では、交換データリストに対してハッシュ値を計算し（ステップＳ１６０１）、内部記憶媒体に格納されている秘密鍵でハッシュ値を暗号化して電子署名を得た後（ステップＳ１６０２）、交換データリストに電子署名を付与して交換データリストファイルとする（ステップＳ１６０３）。

【０１２１】つぎに、図８のステップＳ８０８に示した受取証の作成処理手順について説明する。図１７は、図８のステップＳ８０８に示した受取証の作成処理手順を示すフローチャートである。

【０１２２】同図に示すように、この受取証の作成処理では、受け取った交換データ識別番号と論理窓口番号、交換データ電子署名をあわせて受取内容を作成し（ステップＳ１７０１）、この受取内容に対してはハッシュ値を計算する（ステップＳ１７０２）。

【０１２３】その後、内部記憶媒体に格納されている秘密鍵でハッシュ値を暗号化して電子署名を取得し（ステップＳ１７０３）、受取内容に電子署名を付与して受取証とする（ステップＳ１７０４）。

【０１２４】つぎに、受取証の検証処理について説明する。図１８は受取証の検証処理手順を示すフローチャートである。同図に示すように、まず最初に受け取った受取証から電子署名を取り出すとともに（ステップＳ１８０１）、受け取った受取証から受取内容を取り出し（ステップＳ１８０２）、受取内容に対してハッシュ値を計算する（ステップＳ１８０３）。

【０１２５】その後、内部記憶媒体に格納されている公開鍵で電子署名を復号して検証用ハッシュ値を取得し（ステップＳ１８０４）、ハッシュ値と検証用ハッシュ値とを比較する（ステップＳ１８０５）。その結果、ハッシュ値と検証用ハッシュ値とが異なる場合には（ステップＳ１８０５肯定）、エラー処理をおこなって（ステップＳ１８０６）処理を終了し、両者が一致する場合には（ステップＳ１８０５否定）正常終了する。

【０１２６】（３）交換データ一覧処理

つぎに、図１に示したセキュア情報交換装置１０がおこなう交換データ一覧処理手順について具体的に説明する。図１９は、図１に示したセキュア情報交換装置１０がおこなう交換データ一覧処理手順を示すフローチャートである。

【０１２７】同図に示すように、このセキュア情報交換装置１０は、ユーザのアカウント名、受け取った論理窓口番号、アクセス種別（一覧）を元に窓口アクセス権検査処理をおこない（ステップＳ１９０１）、アクセス権があるか否かを確認する（ステップＳ１９０２）。

【０１２８】そして、アクセス権がない場合には（ステップＳ１９０２否定）、エラー処理をおこなった後に（ステップＳ１９０８）処理を終了し、アクセス権がある場合には（ステップＳ１９０２肯定）、受け取った論理窓口番号に対応する交換データリストファイルを大容量記憶装置１３から読み出し（ステップＳ１９０３）、交換データリスト検証処理をおこなう（ステップＳ１９０４）。

【０１２９】その結果、検証に失敗した場合には（ステップＳ１９０５否定）、エラー処理をおこなった（ステップＳ１９０８）後に、処理を終了し、検証に成功した場合には（ステップＳ１９０５肯定）、交換データリストファイルから交換データ識別番号をすべて取り出し、交換データ識別番号リストを作成し（ステップＳ１９０６）、該交換データ識別番号リストをユーザ側に返す（ステップＳ１９０７）。

【０１３０】（４）リトリーブ処理

つぎに、図１に示したセキュア情報交換装置１０がおこなうリトリーブ処理手順について具体的に説明する。図２０は、図１に示したセキュア情報交換装置１０がおこなうリトリーブ処理手順を示すフローチャートである。この処理は、ユーザから論理窓口番号と交換データ識別番号を受け取る。

【０１３１】同図に示すように、セキュア情報交換装置１０は、ユーザのアカウント名、受け取った論理窓口番号、アクセス種別（リトリーブ）を元に窓口アクセス権検査処理をおこない（ステップＳ２００１）、アクセス権があるか否かを確認する（ステップＳ２００２）。

【０１３２】その結果、アクセス権がない場合には（ステップＳ２００２否定）、エラー処理をおこなった後に（ステップＳ２００８）処理を終了し、アクセス権がある場合には（ステップＳ２００２肯定）、論理窓口番号に対応するディレクトリから交換データ識別番号に対応する交換データを読み出し（ステップＳ２００３）、交換データ識別番号、交換データを元に交換データリスト削除処理をおこない（ステップＳ２００４）、処理が成功したか否かを確認する（ステップＳ２００５）。

【０１３３】そして、処理が失敗した場合には（ステップＳ２００５否定）、エラー処理をおこなった後に（ステップＳ２００８）処理を終了し、処理が成功した場合には（ステップＳ２００５肯定）、交換データファイルを大容量記憶装置１３の論理窓口番号に対応するディレクトリから削除し（ステップＳ２００６）、交換データをユーザに送信する（ステップＳ２００７）。

【０１３４】つぎに、図２０のステップＳ２００４に示した交換データの削除処理手順について説明する。図２１は、図２０のステップＳ２００４に示した交換データの削除処理手順を示すフローチャートである。この処理は、論理窓口番号、交換データ識別番号、交換データを受け取り、交換データリストから該当する交換データエントリを削除するものである。

【０１３５】同図に示すように、この交換データの削除処理では、論理窓口番号に対応する交換データリストファイルを大容量記憶装置１３から読み出し（ステップＳ２１０１）、交換データリスト検証処理をおこない（ステップＳ２１０２）、検証に成功したか否かを確認する（ステップＳ２１０３）。

【０１３６】その結果、検証に失敗した場合には（ステップＳ２１０３否定）、エラー処理をおこなった後に（ステップＳ２１１２）処理を終了し、検証に成功した場合には（ステップＳ２１０３肯定）、受け取った交換データ識別番号に該当する交換データエントリを交換データリストから取得するとともに（ステップＳ２１０４）、交換データエントリから交換データ電子署名を取り出す（ステップＳ２１０５）。

【０１３７】その後、内部記憶媒体に格納されている公開鍵で交換データ電子署名を復号して検証用ハッシュ値とするとともに（ステップＳ２１０６）、受け取った交換データについてのハッシュ値を計算し（ステップＳ２１０７）、ハッシュ値と検証法ハッシュ値が一致するか否かを確認する（ステップＳ２１０８）。

【０１３８】その結果、両者が一致しない場合には（ステップＳ２１０８否定）、エラー処理をおこなった後に（ステップＳ２１１２）処理を終了し、両者が一致する場合には（ステップＳ２１０８肯定）、交換データリストから先の交換データエントリを削除し（ステップＳ２１０９）、交換データリスト署名処理をおこなった後に（ステップＳ２１１０）、大容量記憶装置２１１１に交換データリストファイルを格納する（ステップＳ２１１１）。

【０１３９】（５）送出確認処理

つぎに、図１に示したセキュア情報交換装置１０がおこなう送出確認処理手順について具体的に説明する。図２２は、図１に示したセキュア情報交換装置１０がおこなう送出確認処理手順を示すフローチャートである。この処理は、ユーザから受取証を受け取り、これに対応する交換データが他方のネットワークに送出されたかどうかを確認するものである。

【０１４０】同図に示すように、このセキュア情報交換装置１０では、受け取った受取証を元に受取証検証処理をおこない（ステップＳ２２０１）、検証に成功したか否かを確認する（ステップＳ２２０２）。

【０１４１】その結果、検証に失敗した場合（ステップＳ２２０２否定）には、エラー処理をおこなった後に（ステップＳ２２１２）処理を終了し、検証に成功した場合には（ステップＳ２２０２肯定）、受取証から受取内容を取り出し（ステップＳ２２０３）、この受取内容から論理窓口番号と交換データ識別番号を取り出す（ステップＳ２２０４）。

【０１４２】その後、大容量記憶装置１３から論理窓口番号に対応する交換データリストファイルを読み出し（ステップＳ２２０５）、交換データリスト検証処理をおこなった後に（ステップＳ２２０６）、検証に成功したか否かを確認する（ステップＳ２２０７）。

【０１４３】その結果、検証に失敗した場合（ステップＳ２２０７否定）には、エラー処理をおこなった（ステップＳ２２１２）後に、処理を終了する。一方、検証に成功した場合には（ステップＳ２２０７肯定）、交換データリストファイルから交換データ識別番号に対応する交換データエントリを取り出し（ステップＳ２２０８）、対応する交換データエントリが存在するか否かを確認する（ステップＳ２２０９）。

【０１４４】そして、対応する交換データエントリが存在する場合（ステップＳ２２０９肯定）には、交換データは他方のネットワークに送出されていないことをユーザに通知し（ステップＳ２２１０）、対応する交換データエントリが存在しない場合には（ステップＳ２２０９否定）、交換データが他方のネットワークに送出されたことをユーザに通知する（ステップＳ２２１１）。

【０１４５】上述してきたように、本実施の形態では、外部用モジュール１０ａが外部ネットワーク１から交換データを受け付けた際に、該交換データを大容量記憶装置１３に格納し、内部用モジュール１０ｂが内部ネットワーク２から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを大容量記憶装置１３から取り出して出力するセキュア情報交換装置１０を設けるよう構成したので人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうことができる。

【０１４６】なお、一般的な情報システムがおこなうように、処理した内容をログとして記録することもできる。この場合には、記録したログをデータ交換をおこなった証拠とできるよう、交換データと同様にログにも電子署名を施すことが望ましい。

【０１４７】また、場合によっては、送出確認だけでなく、送信取消の処理をおこなうよう構成することもできる。また、交換データが大容量記憶装置１０に格納されている間に、交換データを送り込んだユーザが受取証を提示して送信取消を要求した場合には、装置内部に保持した交換データを取り消すように構成することになる。

【０１４８】なお、取り消されたのか、他方のネットワークに送出したのかを明確にするために、取り消した交換データについては別途取消リストのようなもので管理する必要がある。

【０１４９】また、交換データをストアする際に、その交換データに対して保持期限を設定できるようにすることもできる。その保持期限を過ぎてもリトリーブされない場合には、保持期限が過ぎたことをストアしたユーザに通知したうえでその交換データを削除することになる。

【０１５０】また、一方のネットワークにある原本性保

証電子保存システムから電子原本を受け取り、他方のネットワークからその電子原本の受取要求があれば、その電子原本をその他方のネットワークにある原本性保証電子保存システムに送出するよう構成することもできる。

【０１５１】なお、本実施の形態で説明したセキュア情報交換方法は、あらかじめ用意されたプログラムをパーソナルコンピュータやワークステーションなどのコンピュータで実行することによって実現される。このプログラムは、ＨＤ（ハードディスク）、ＦＤ（フロッピーディスク）、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって、実行される。また、このプログラムは、インターネットなどのネットワークを介して配布することが可能な伝送媒体であってもよい。

【０１５２】

【発明の効果】以上説明したように、請求項１に記載の発明によれば、第１の端末装置から交換データを受け付けた際に、該交換データを記憶手段に格納し、第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを記憶手段から取り出して当該第２の端末装置に出力するセキュア情報交換装置を第１のネットワークおよび第２のネットワークの間に配設するよう構成したので、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうことが可能なセキュア情報交換システムが得られるという効果を奏する。

【０１５３】また、請求項２に記載の発明によれば、第１のモジュールでは、第１の端末装置から交換データを受け付け、受け付けた交換データについての第１の改ざん検知コードを算定し、算定した第１の改ざん検知コードを当該交換データと対応づけて記憶手段に格納し、第２のモジュールでは、第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第１の改ざん検知コードを記憶手段から取り出し、取り出した第１の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証するよう構成したので、交換データの改ざんを防止することが可能なセキュア情報交換システムが得られるという効果を奏する。

【０１５４】また、請求項３に記載の発明によれば、第１のモジュールでは、複数の交換データを含むリストについての第２の改ざん検知コードを算定し、算定した第２の改ざん検知コードをリストとともに記憶手段に格納し、第２のモジュールでは、第２の改ざん検知コードに基づいてリストの改ざんの有無を検証するよう構成したので、交換データをリスト構造で格納する場合にも、このリストの改ざんを効率よく防止することが可能なセキュア情報交換システムが得られるという効果を奏する。

【０１５５】また、請求項４に記載の発明によれば、第１のモジュールおよび第２のモジュールが、記憶手段に記憶した交換データの編集要求並びに削除要求を拒否するよう構成したので、交換データが編集や削除される被害を防止することが可能なセキュア情報交換システムが得られるという効果を奏する。

【０１５６】また、請求項５に記載の発明によれば、第１の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成し、作成した受取証データを第１の端末装置に返送するよう構成したので、交換データの受付を効率よく証明することができるとともに、該交換データの授受にかかる責任の所在を明らかにすることが可能なセキュア情報交換システムが得られるという効果を奏する。

【０１５７】また、請求項６に記載の発明によれば、交換データの特徴量を含む受取証データを作成するよう構成したので、交換データと受取証の不整合を効率よく防止することが可能なセキュア情報交換システムが得られるという効果を奏する。

【０１５８】また、請求項７に記載の発明によれば、交換データを特定する識別情報を含む受取証データを作成するよう構成したので、該当する交換データを効率よく記憶手段から検索することが可能なセキュア情報交換システムが得られるという効果を奏する。

【０１５９】また、請求項８に記載の発明によれば、受取証データの受取内容についての第３の改ざん検知コードを生成し、該生成した第３の改ざん検知コードを含む受取証データを作成するよう構成したので、この受取証データ自体の改ざんについても防止することが可能なセキュア情報交換システムが得られるという効果を奏する。

【０１６０】また、請求項９に記載の発明によれば、第１の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが第２の端末装置に送出済みであるか否かを確認し、この確認結果を第１の端末装置に通知するよう構成したので、送信確認を効率よくおこなうことが可能なセキュア情報交換システムが得られるという効果を奏する。

【０１６１】また、請求項１０に記載の発明によれば、第１の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが記憶手段に記憶されているか否かを確認し、記憶手段に当該交換データが記憶されていることが確認された際に、当該交換データを記憶手段から削除し、交換データの削除の有無を第１の端末装置に通知するよう構成したので、誤って交換データを送信した場合であっても、該交換データの送信を効率よく取り消すことが可能なセキュア情報交換システムが得られるという効果を奏する。

【０１６２】また、請求項１１に記載の発明によれば、第１の改ざん検知コード、第２の改ざん検知コードまたは第３の検知コードを、装置内部に保持した秘密鍵を用

いて算定した電子署名とするよう構成したので、迅速かつ効率よく改ざんを防止することが可能なセキュア情報交換システムが得られるという効果を奏する。

【０１６３】また、請求項１２に記載の発明によれば、第１のモジュールおよび第２のモジュールを耐タンパー性を有する筐体に格納するよう構成したので、該第１のモジュールおよび第２のモジュール自体に対する不正な行為を防止することが可能なセキュア情報交換システムが得られるという効果を奏する。

【０１６４】また、請求項１３に記載の発明によれば、第１の端末装置から交換データを受け付けた際に、該交換データを記憶部に格納し、第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データを記憶部から取り出して当該第２の端末装置に出力するよう構成したので、人的労力の負担軽減並びにネットワークの独立性を図りつつ、ネットワーク間の情報交換を効率よくおこなうことが可能なセキュア情報交換方法が得られるという効果を奏する。

【０１６５】また、請求項１４に記載の発明によれば、第１の端末装置から交換データを受け付け、受け付けた交換データについての第１の改ざん検知コードを算定し、算定した第１の改ざん検知コードを当該交換データと対応づけて記憶部に格納し、一方、第２の端末装置から交換データの取り出し要求を受け付けた際に、該取り出し要求に対応する交換データおよび第１の改ざん検知コードを記憶部から取り出し、取り出した第１の改ざん検知コードに基づいて当該交換データの改ざんの有無を検証するよう構成したので、交換データの改ざんを防止することが可能なセキュア情報交換方法が得られるという効果を奏する。

【０１６６】また、請求項１５に記載の発明によれば、複数の交換データを含むリストについての第２の改ざん検知コードを算定し、算定した第２の改ざん検知コードをリストとともに記憶部に格納し、第２のモジュールでは、第２の改ざん検知コードに基づいてリストの改ざんの有無を検証するよう構成したので、交換データをリスト構造で格納する場合にも、このリストの改ざんを効率よく防止することが可能なセキュア情報交換方法が得られるという効果を奏する。

【０１６７】また、請求項１６に記載の発明によれば、記憶部に記憶した交換データの編集要求並びに削除要求を拒否できるとしたので、交換データが編集や削除される被害を防止することが可能なセキュア情報交換方法が得られるという効果を奏する。

【０１６８】また、請求項１７に記載の発明によれば、第１の端末装置から交換データを受け付けた際に、該交換データの受け取りを証明する受取証データを作成し、作成した受取証データを第１の端末装置に返送するよう構成したので、交換データの受付を効率よく証明することができるとともに、該交換データの授受にかかる責任の所在を明らかにすることが可能なセキュア情報交換方法が得られるという効果を奏する。

【０１６９】また、請求項１８に記載の発明によれば、交換データの特徴量を含む受取証データを作成するよう構成したので、交換データと受取証の不整合を効率よく防止することが可能なセキュア情報交換方法が得られるという効果を奏する。

【０１７０】また、請求項１９に記載の発明によれば、交換データを特定する識別情報を含む受取証データを作成するよう構成したので、該当する交換データを効率よく記憶手段から検索することが可能なセキュア情報交換方法が得られるという効果を奏する。

【０１７１】また、請求項２０に記載の発明によれば、受取証データの受取内容についての第３の改ざん検知コードを生成し、該生成した第３の改ざん検知コードを含む受取証データを作成するよう構成したので、この受取証データ自体の改ざんについても防止することが可能なセキュア情報交換方法が得られるという効果を奏する。

【０１７２】また、請求項２１に記載の発明によれば、第１の端末装置から受取証データおよび送信確認要求を受け付けた際に、該受取証データに対応する交換データが第２の端末装置に送出済みであるか否かを確認し、この確認結果を第１の端末装置に通知するよう構成したので、送信確認を効率よくおこなうことが可能なセキュア情報交換方法が得られるという効果を奏する。

【０１７３】また、請求項２２に記載の発明によれば、第１の端末装置から受取証データおよび送信取消要求を受け付けた際に、該受取証データに対応する交換データが記憶部に記憶されているか否かを確認し、記憶部に当該交換データが記憶されていることが確認された際に、当該交換データを記憶部から削除し、交換データの削除の有無を第１の端末装置に通知するよう構成したので、誤って交換データを送信した場合であっても、該交換データの送信を効率よく取り消すことが可能なセキュア情報交換方法が得られるという効果を奏する。

【０１７４】また、請求項２３に記載の発明によれば、第１の改ざん検知コード、第２の改ざん検知コードまたは第３の検知コードを、装置内部に保持した秘密鍵を用いて算定した電子署名とするよう構成したので、迅速かつ効率よく改ざんを防止することが可能なセキュア情報交換方法が得られるという効果を奏する。

【０１７５】また、請求項２４に記載の発明によれば、請求項１３～２３のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムを機械読み取り可能となり、これによって、請求項１３～２３のいずれか一つの動作をコンピュータによって実現することが可能な記録媒体が得られるという効果を奏する。

【図面の簡単な説明】

【図１】この発明の本実施の形態で用いるセキュア情報

交換システムの概念を説明するための説明図である。

【図２】この発明の本実施の形態の図１に示したセキュア情報交換装置の配置位置の一例を示す説明図である。

【図３】この発明の本実施の形態の図１に示したセキュア情報交換装置の装置構成を示すブロック図である。

【図４】この発明の本実施の形態の図１に示したセキュア情報交換装置の処理内容の一覧を示す説明図である。

【図５】この発明の本実施の形態の図１に示したセキュア情報交換装置がおこなうサービス受け付け処理手順を示すフローチャートである。

【図６】この発明の本実施の形態の図５のステップＳ５０３に示したユーザ認証処理手順を示すフローチャートである。

【図７】この発明の本実施の形態のセキュア情報交換装置のアカウント管理データの構成を示す説明図である。

【図８】この発明の本実施の形態の図１に示したセキュア情報交換装置がおこなうストア処理手順を示すフローチャートである。

【図９】この発明の本実施の形態のセキュア情報交換装置のストア処理の概念を説明するための説明図である。

【図１０】この発明の本実施の形態の交換データリストファイルの構造を示す説明図である。

【図１１】この発明の本実施の形態のセキュア情報交換装置の受取証データの構造を示す説明図である。

【図１２】この発明の本実施の形態の図８のステップＳ８０１に示した窓口アクセス権検査処理手順を示すフローチャートである。

【図１３】この発明の本実施の形態のセキュア情報交換装置の論理窓口管理データの構造を示す説明図である。

【図１４】この発明の本実施の形態の図８のステップＳ８０５に示した交換データリスト追加処理手順を示すフローチャートである。

【図１５】この発明の本実施の形態の図１４のステップＳ１４０２に示した交換データリスト検証処理手順を示すフローチャートである。

【図１６】この発明の本実施の形態の図１４のステップＳ１４０６に示した交換データリスト署名処理手順を示すフローチャートである。

【図１７】この発明の本実施の形態の図８のステップＳ８０８に示した受取証の作成処理手順を示すフローチャートである。

【図１８】この発明の本実施の形態の受取証の検証処理手順を示すフローチャートである。

【図１９】この発明の本実施の形態の図１に示したセキュア情報交換装置がおこなう交換データ一覧処理手順を示すフローチャートである。

【図２０】この発明の本実施の形態の図１に示したセキュア情報交換装置がおこなうリトリーブ処理手順を示すフローチャートである。

【図２１】この発明の本実施の形態の図２０のステップＳ２００４に示した交換データの削除処理手順を示すフローチャートである。

【図２２】この発明の本実施の形態の図１に示したセキュア情報交換装置がおこなう送出確認処理手順を示すフローチャートである。

【図２３】従来の典型的なファイアウオールの概念を説明するための説明図である。

【符号の説明】

１　外部ネットワーク
２　内部ネットワーク
１０　セキュア情報交換装置
１０ａ　外部モジュール
１０ｂ　内部モジュール
１１　コンピュータ
１１，１２　端末装置
１３　大容量記憶装置
２０　住民基本台帳ネットワーク
１００　耐タンパー筐体
１００　筐体
１１０，１２０　通信ポート
１１１，１２１　一時記憶部
１１２，１２２　内部記憶媒体
１１３，１２３　プロセッサ
１１４，１２４　内部タイマ
１１５，１２５　プログラム格納媒体

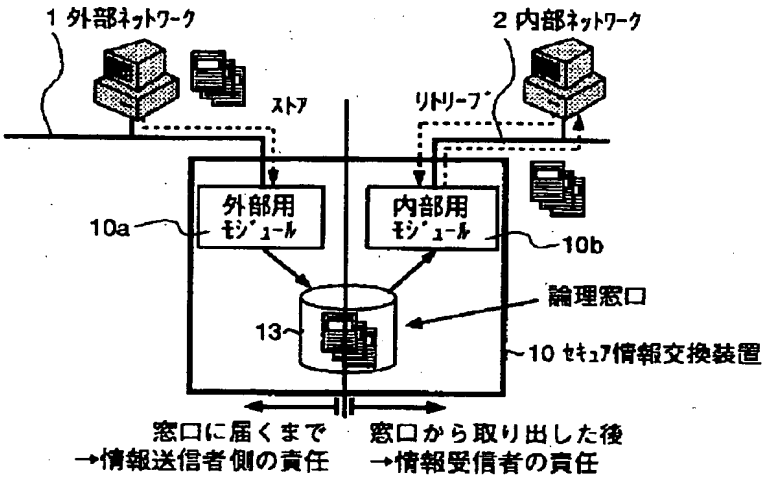
【図７】

ｱｶｳﾝﾄｴﾝﾄﾘ＃１	ｱｶｳﾝﾄ名
	ﾊﾟｽﾜｰﾄﾞ
ｱｶｳﾝﾄｴﾝﾄﾘ＃２	
・・・	
ｱｶｳﾝﾄｴﾝﾄﾘ＃Ｎ	

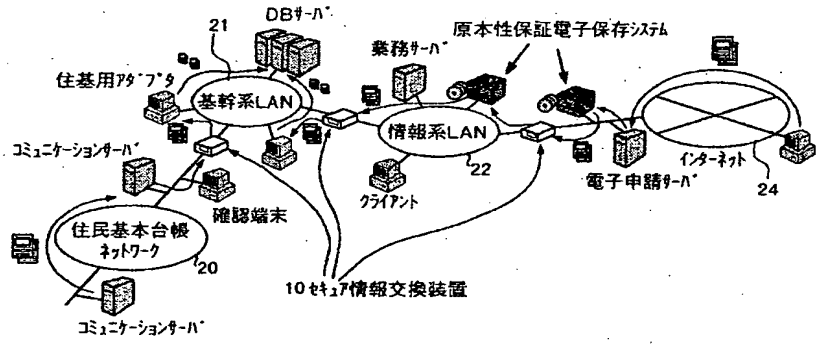
【図１１】

受取内容	交換ﾃﾞｰﾀ識別番号
	格納した論理窓口番号
	交換ﾃﾞｰﾀ電子署名
受取内容に対する電子署名	

【図１】



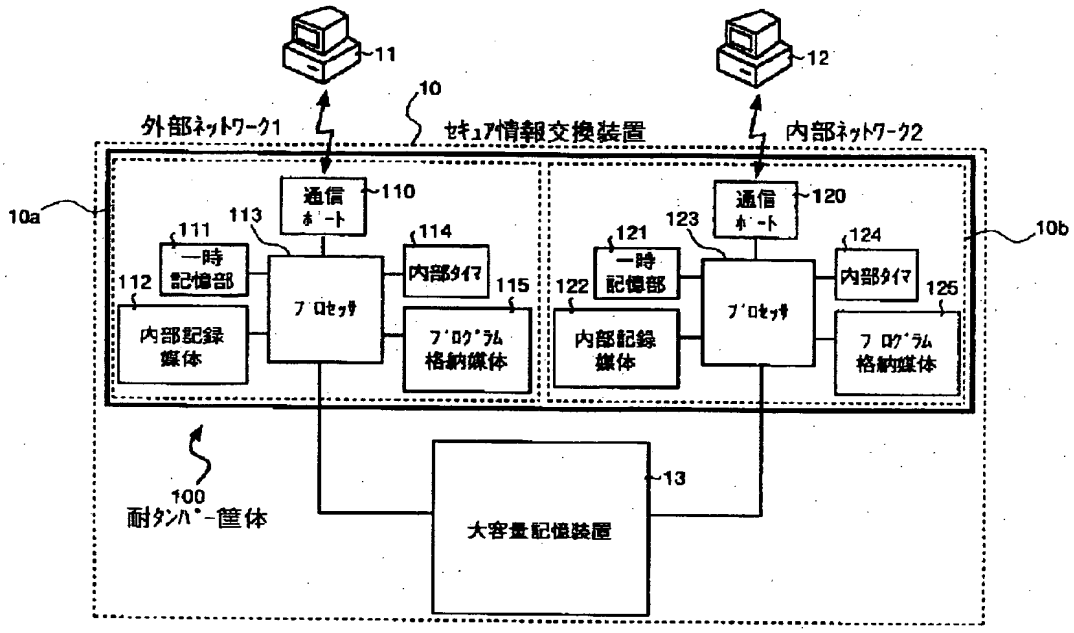
【図２】



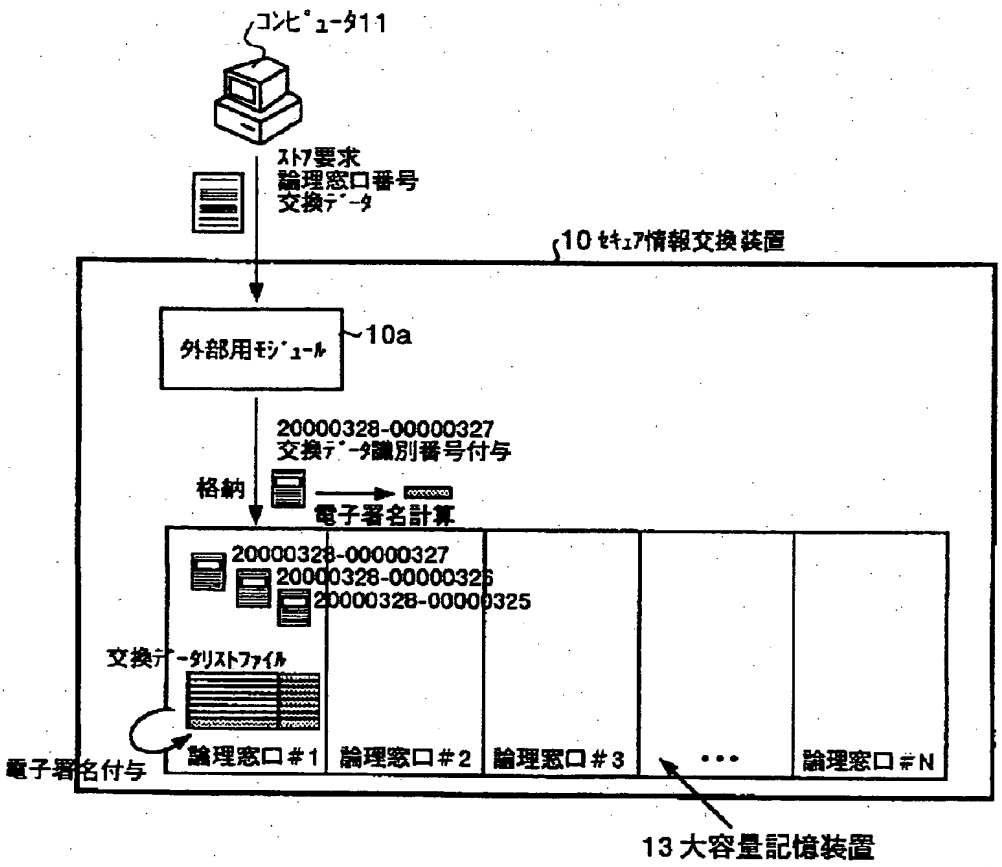
【図４】

処理名	処理内容
サービス受付処理	セキュア情報交換装置にアクセスするユーザから様々なサービス処理要求を受け付け、その要求内容に応じて処理を割り振るものである。
ストア処理	セキュア情報交換装置に対して送信された交換データを受け取ってシステム内部にストアする処理である。
交換データ一覧処理	セキュア情報交換装置内部で保持している交換データの識別番号の一覧を取得する処理である。
リトリーブ処理	セキュア情報交換装置に対して送られた取り出し要求に対して、システム内部に保持されている交換データを送出する処理である。
送出確認処理	セキュア情報交換装置に対して送信された交換データが、すでに他方のネットワークで取り出されたかどうか確認する処理である。

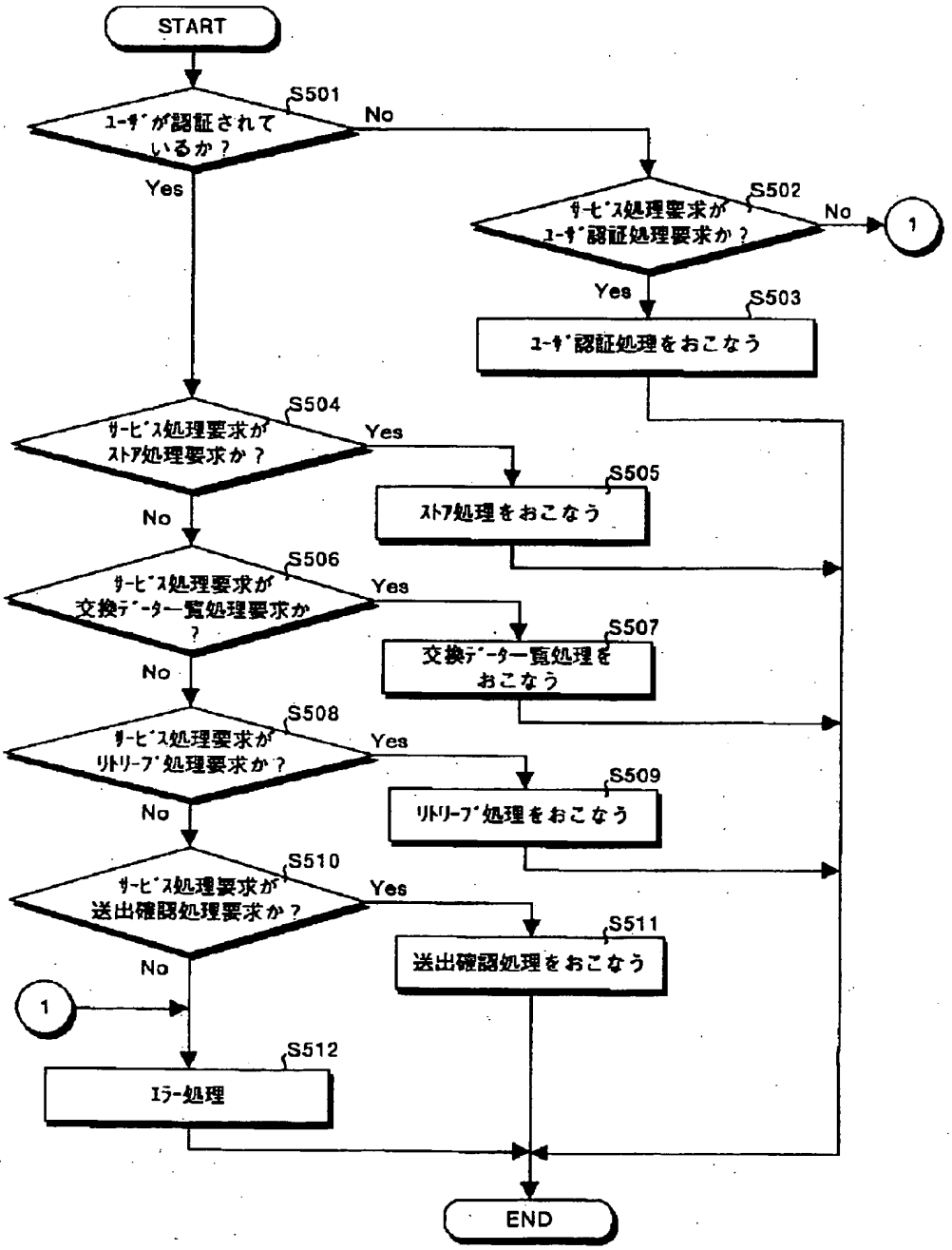
【図３】


11
12
10
外部ネットワーク1
セキュア情報交換装置
内部ネットワーク2
10a
10b
通信ポート
110
111
一時記憶部
113
114
内部タイマ
112
内部記録媒体
プロセッサ
115
プログラム格納媒体
通信ポート
120
121
一時記憶部
123
124
内部タイマ
122
内部記録媒体
プロセッサ
125
プログラム格納媒体
100
耐タンパー筐体
13
大容量記憶装置

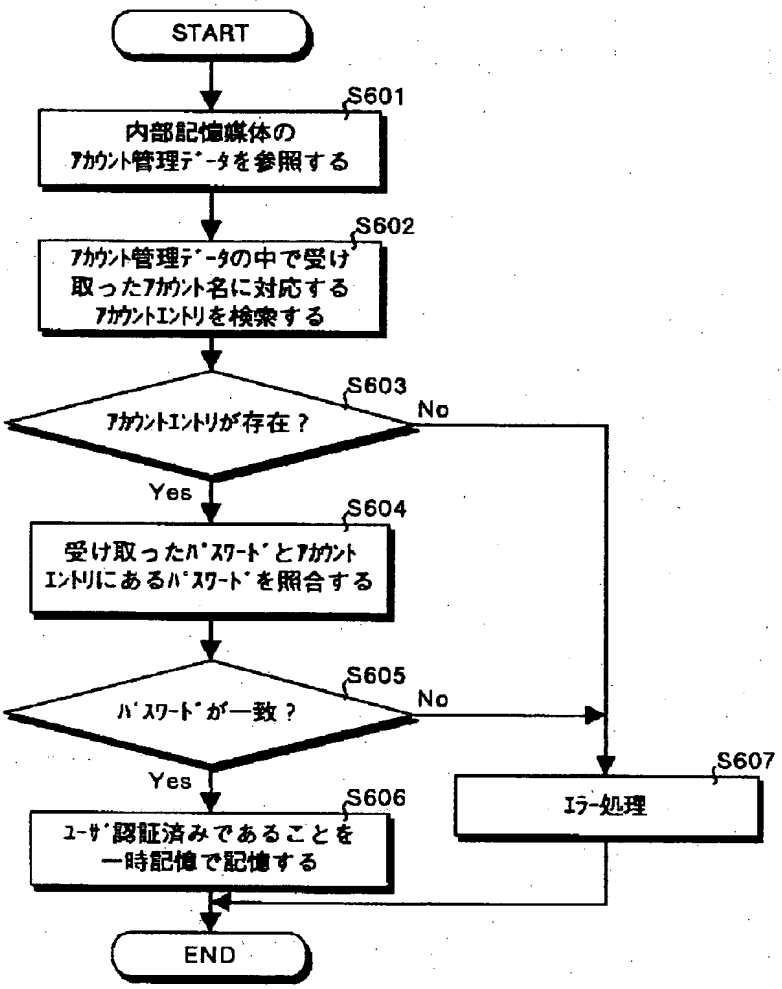
【図９】


コンピュータ11
ストア要求
論理窓口番号
交換データ
10 セキュア情報交換装置
外部用モジュール
10a
20000328-00000327
交換データ識別番号付与
格納
電子署名計算
20000328-00000327
20000328-00000326
20000328-00000325
交換データリストファイル
電子署名付与
論理窓口＃1
論理窓口＃2
論理窓口＃3
・・・
論理窓口＃N
13 大容量記憶装置

【図５】


START
S501
ﾕｰｻﾞｰが認証されているか？
No
Yes
S502
ｻｰﾋﾞｽ処理要求がﾕｰｻﾞｰ認証処理要求か？
No
1
Yes
S503
ﾕｰｻﾞｰ認証処理をおこなう
S504
ｻｰﾋﾞｽ処理要求がｽﾄｱ処理要求か？
Yes
S505
ｽﾄｱ処理をおこなう
No
S506
ｻｰﾋﾞｽ処理要求が交換ﾃﾞｰﾀｰ一覧処理要求か？
Yes
S507
交換ﾃﾞｰﾀｰ一覧処理をおこなう
No
S508
ｻｰﾋﾞｽ処理要求がﾘﾄﾘｰﾌﾞ処理要求か？
Yes
S509
ﾘﾄﾘｰﾌﾞ処理をおこなう
No
S510
ｻｰﾋﾞｽ処理要求が送出確認処理要求か？
Yes
S511
送出確認処理をおこなう
No
1
S512
ｴﾗｰ処理
END

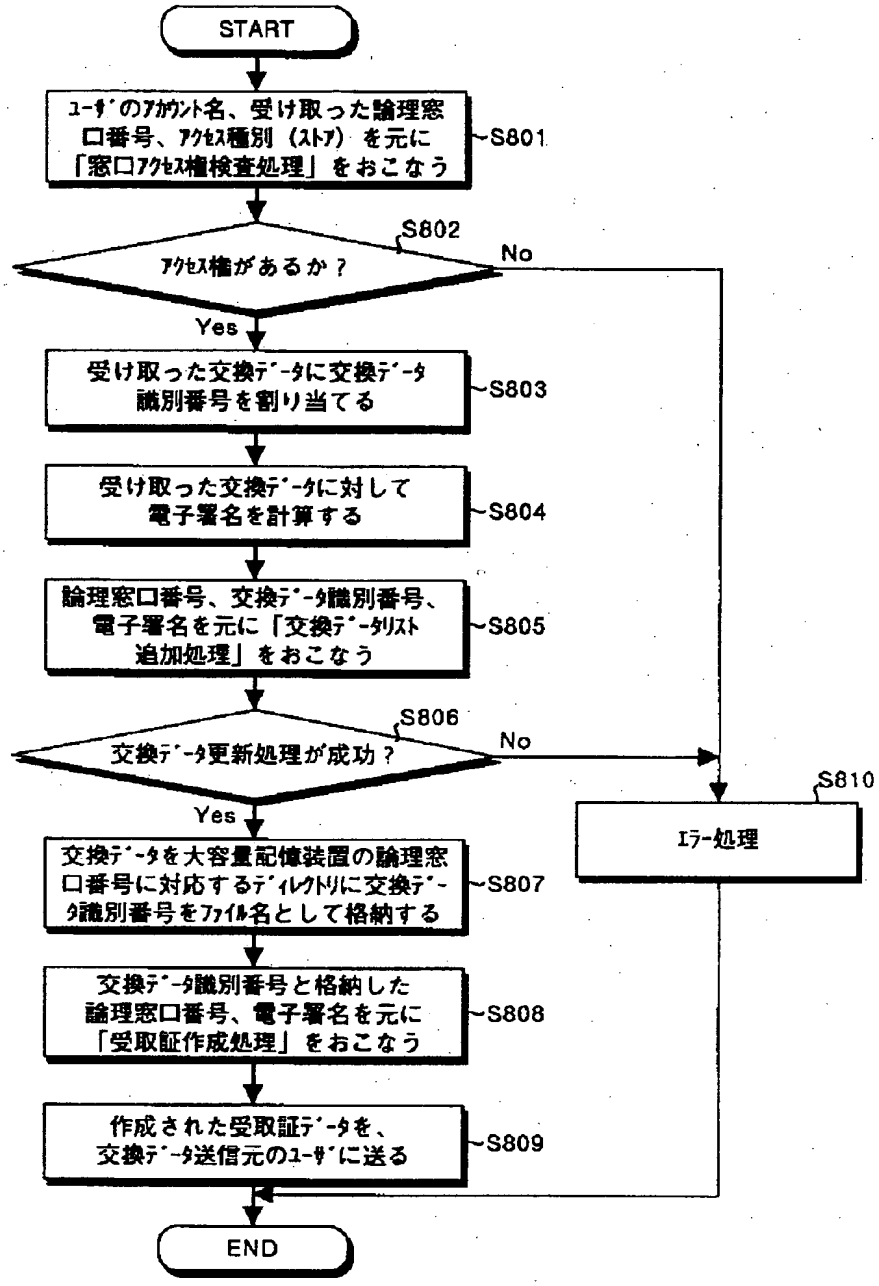
【図６】



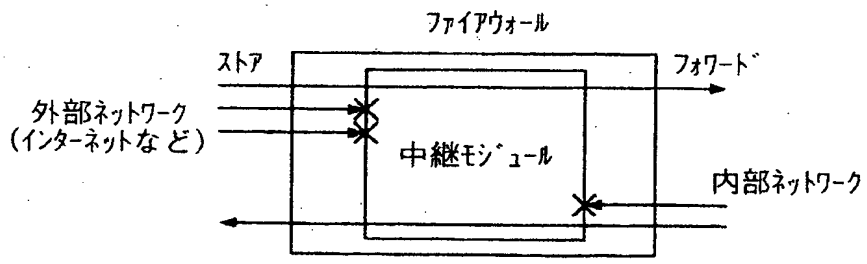
【図１０】

交換ﾃﾞｰﾀﾘｽﾄ	交換ﾃﾞｰﾀｴﾝﾄﾘ＃１	交換ﾃﾞｰﾀ識別番号
		交換ﾃﾞｰﾀ電子署名
	交換ﾃﾞｰﾀｴﾝﾄﾘ＃２	
	・・・	
	交換ﾃﾞｰﾀｴﾝﾄﾘ＃Ｎ	
交換ﾃﾞｰﾀﾘｽﾄに対する電子署名		

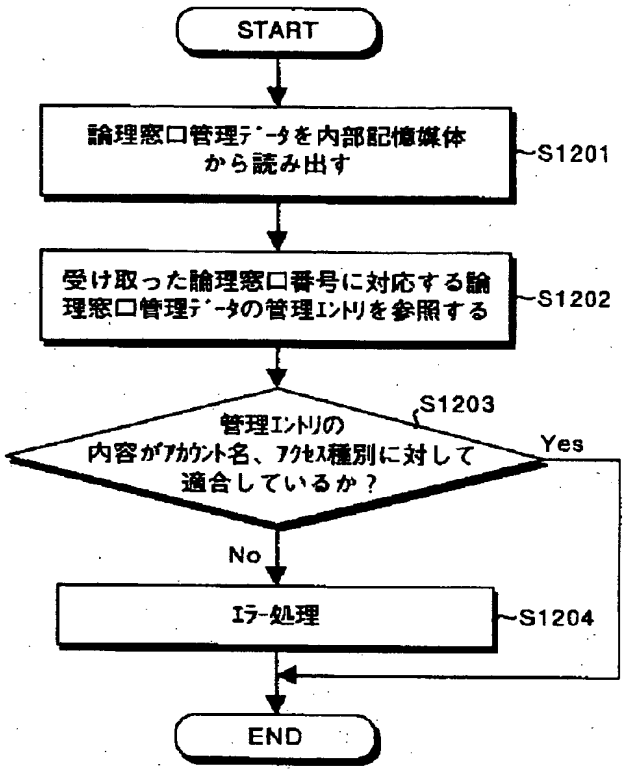
【図８】


START
ユーザのアカウント名、受け取った論理窓口番号、アクセス種別（ストア）を元に「窓口アクセス権検査処理」をおこなう
S801
S802
アクセス権があるか？
No
Yes
受け取った交換データに交換データ識別番号を割り当てる
S803
受け取った交換データに対して電子署名を計算する
S804
論理窓口番号、交換データ識別番号、電子署名を元に「交換データリスト追加処理」をおこなう
S805
S806
交換データ更新処理が成功？
No
Yes
S810
エラー処理
交換データを大容量記憶装置の論理窓口番号に対応するディレクトリに交換データ識別番号をファイル名として格納する
S807
交換データ識別番号と格納した論理窓口番号、電子署名を元に「受取証作成処理」をおこなう
S808
作成された受取証データを、交換データ送信元のユーザに送る
S809
END

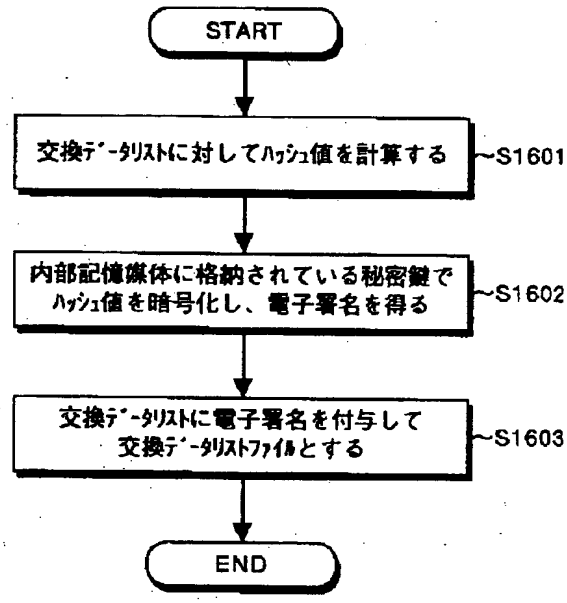
【図２３】


ファイアウォール
ストア
フォワード
外部ネットワーク
（インターネットなど）
中継モジュール
内部ネットワーク

【図１２】



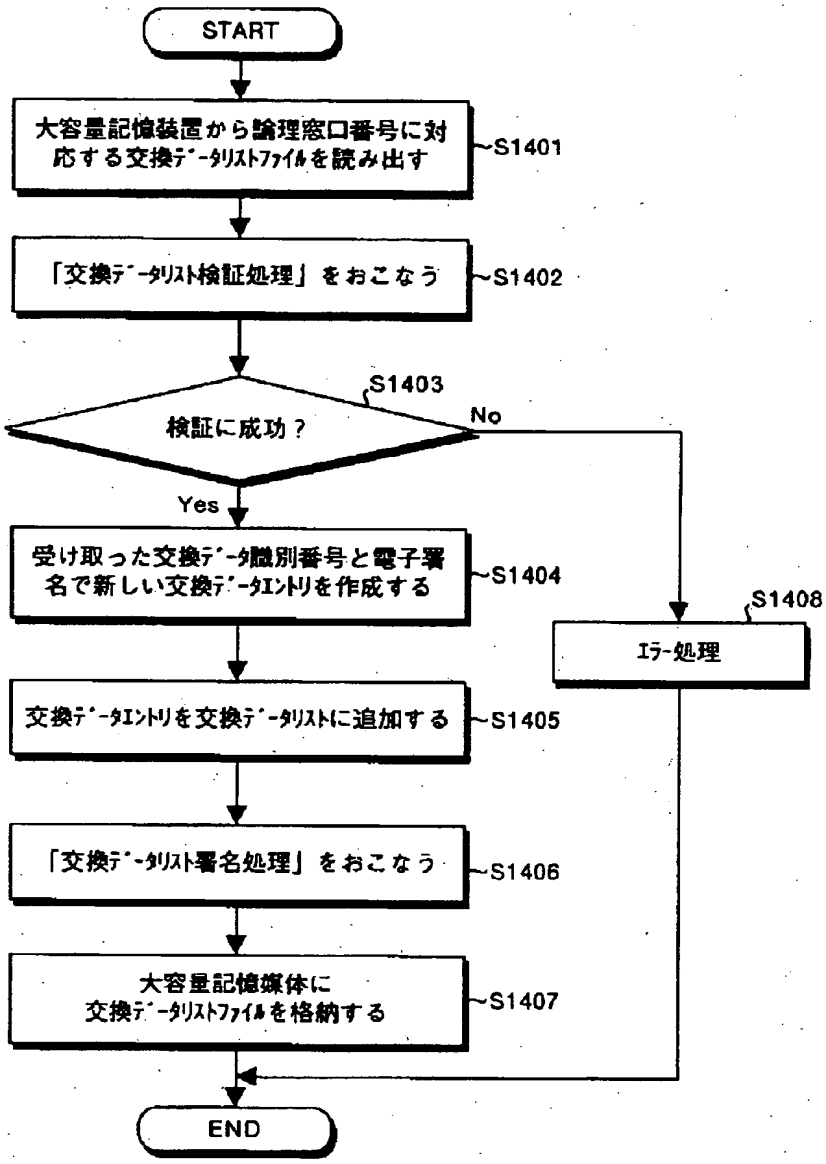
【図１６】



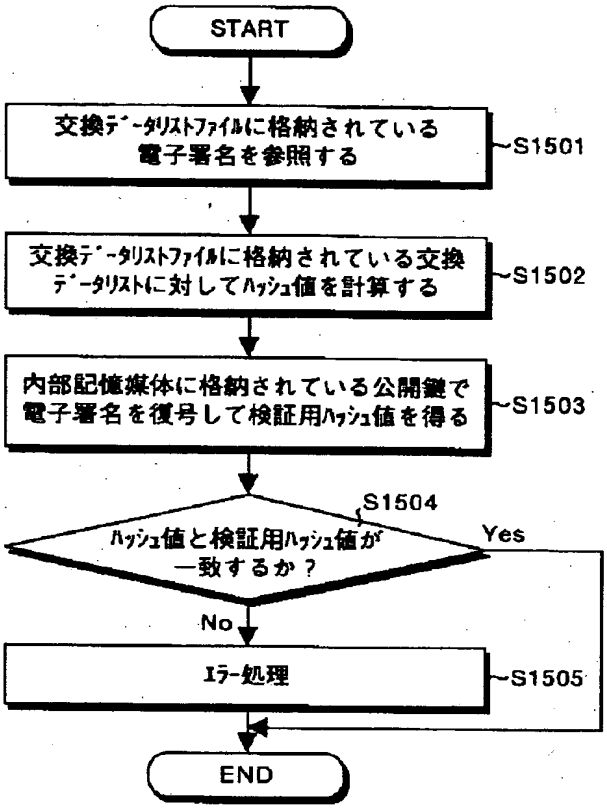
【図１３】

管理ｴﾝﾄﾘ＃１	論理窓口番号		
	ﾃﾞｰﾀ交換方向		
	ｱｸｾｽ許可ﾘｽﾄ	ｱｸｾｽ許可ｴﾝﾄﾘ＃１	ｱｶｳﾝﾄ名
		ｱｸｾｽ許可ｴﾝﾄﾘ＃２	
		・・・	
		ｱｸｾｽ許可ｴﾝﾄﾘ＃Ｎ	
管理ｴﾝﾄﾘ＃２			
・・・			
管理ｴﾝﾄﾘ＃Ｎ			

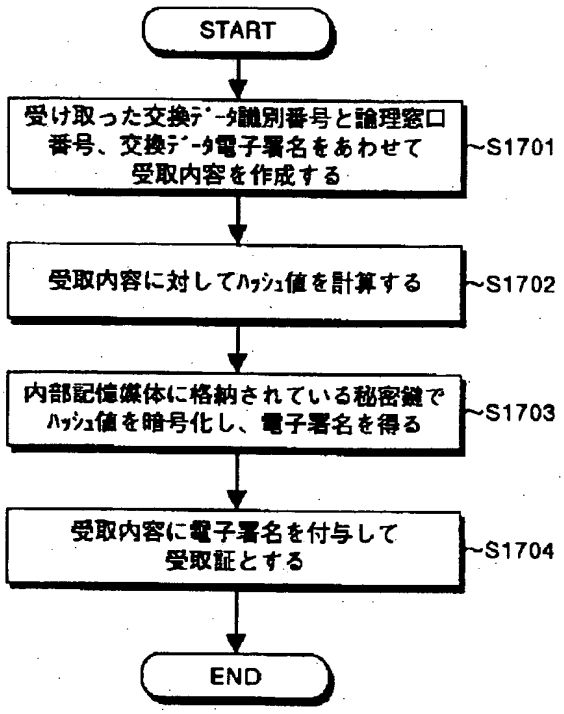
【図１４】


START
大容量記憶装置から論理窓口番号に対応する交換ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙを読み出す
S1401
「交換ﾃﾞｰﾀﾘｽﾄ検証処理」をおこなう
S1402
S1403
検証に成功？
No
Yes
受け取った交換ﾃﾞｰﾀ識別番号と電子署名で新しい交換ﾃﾞｰﾀｴﾝﾄﾘを作成する
S1404
S1408
ｴﾗｰ処理
交換ﾃﾞｰﾀｴﾝﾄﾘを交換ﾃﾞｰﾀﾘｽﾄに追加する
S1405
「交換ﾃﾞｰﾀﾘｽﾄ署名処理」をおこなう
S1406
大容量記憶媒体に交換ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙを格納する
S1407
END

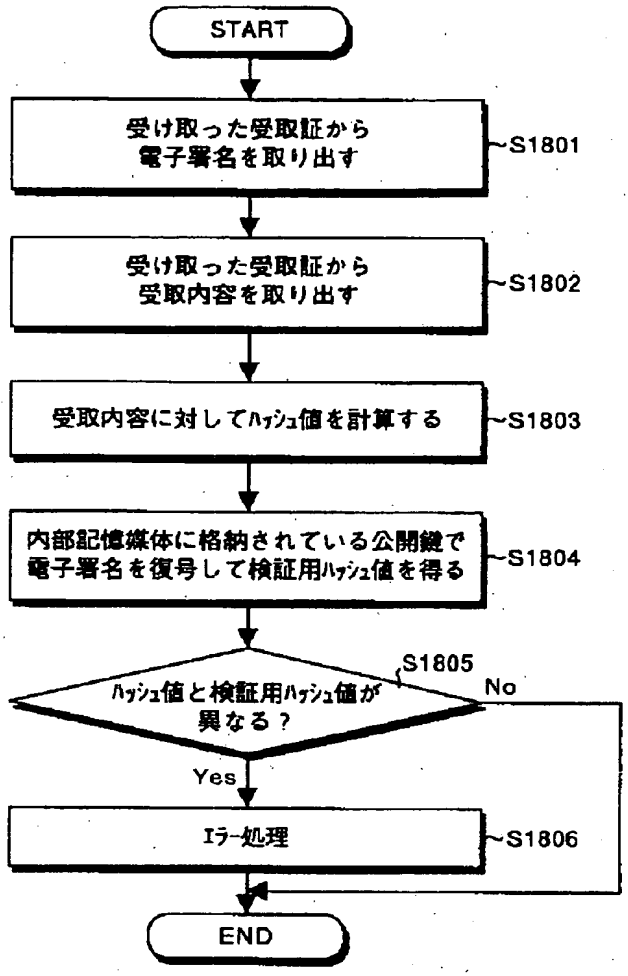
【図１５】


START
交換ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙに格納されている電子署名を参照する
S1501
交換ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙに格納されている交換ﾃﾞｰﾀﾘｽﾄに対してﾊｯｼｭ値を計算する
S1502
内部記憶媒体に格納されている公開鍵で電子署名を復号して検証用ﾊｯｼｭ値を得る
S1503
S1504
ﾊｯｼｭ値と検証用ﾊｯｼｭ値が一致するか？
Yes
No
ｴﾗｰ処理
S1505
END

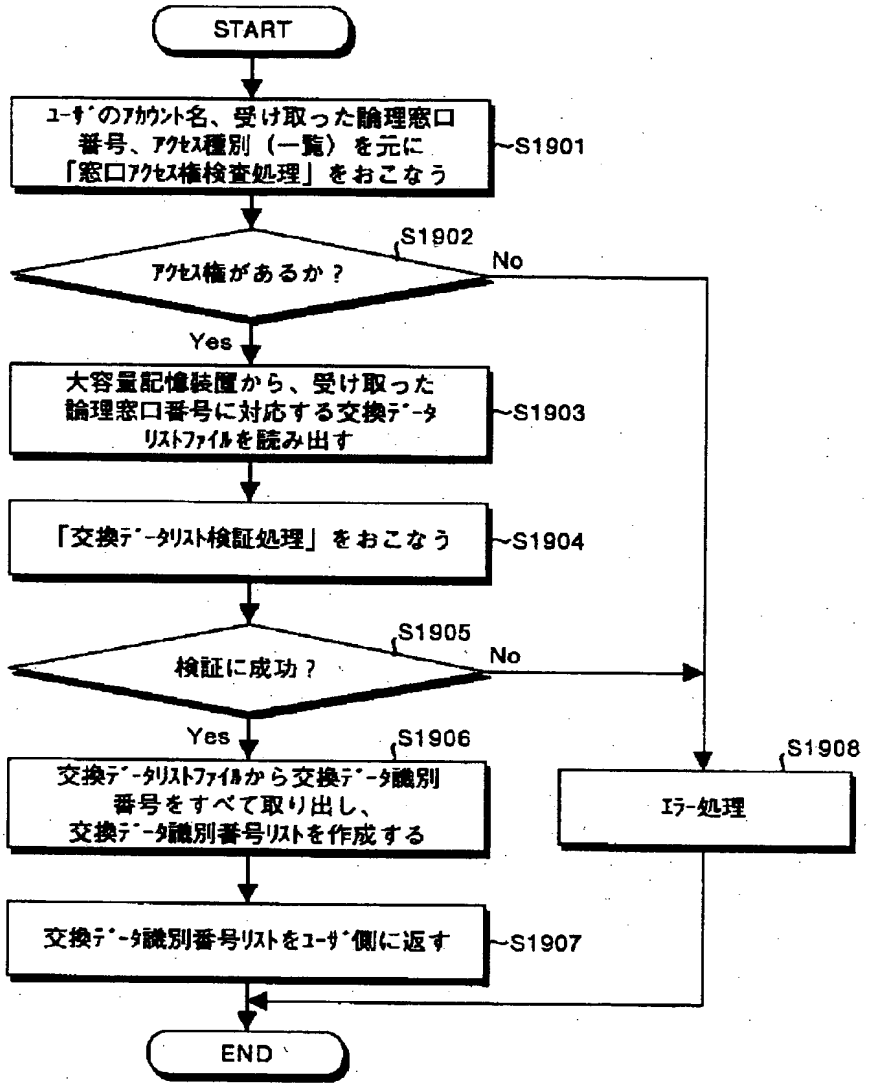
【図１７】


START
受け取った交換ﾃﾞｰﾀ識別番号と論理窓口番号、交換ﾃﾞｰﾀ電子署名をあわせて受取内容を作成する
S1701
受取内容に対してﾊｯｼｭ値を計算する
S1702
内部記憶媒体に格納されている秘密鍵でﾊｯｼｭ値を暗号化し、電子署名を得る
S1703
受取内容に電子署名を付与して受取証とする
S1704
END

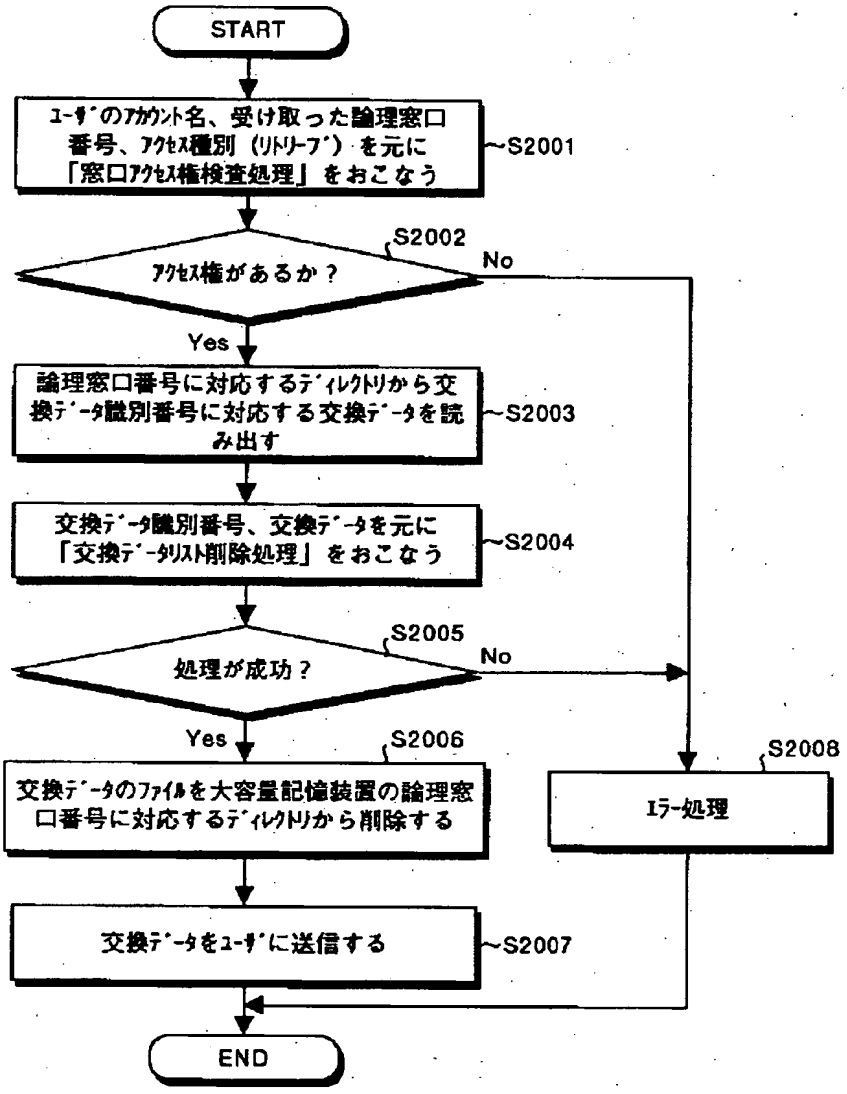
【図１８】


START
受け取った受取証から
電子署名を取り出す
S1801
受け取った受取証から
受取内容を取り出す
S1802
受取内容に対してﾊｯｼｭ値を計算する
S1803
内部記憶媒体に格納されている公開鍵で
電子署名を復号して検証用ﾊｯｼｭ値を得る
S1804
S1805
ﾊｯｼｭ値と検証用ﾊｯｼｭ値が
異なる？
No
Yes
ｴﾗｰ処理
S1806
END

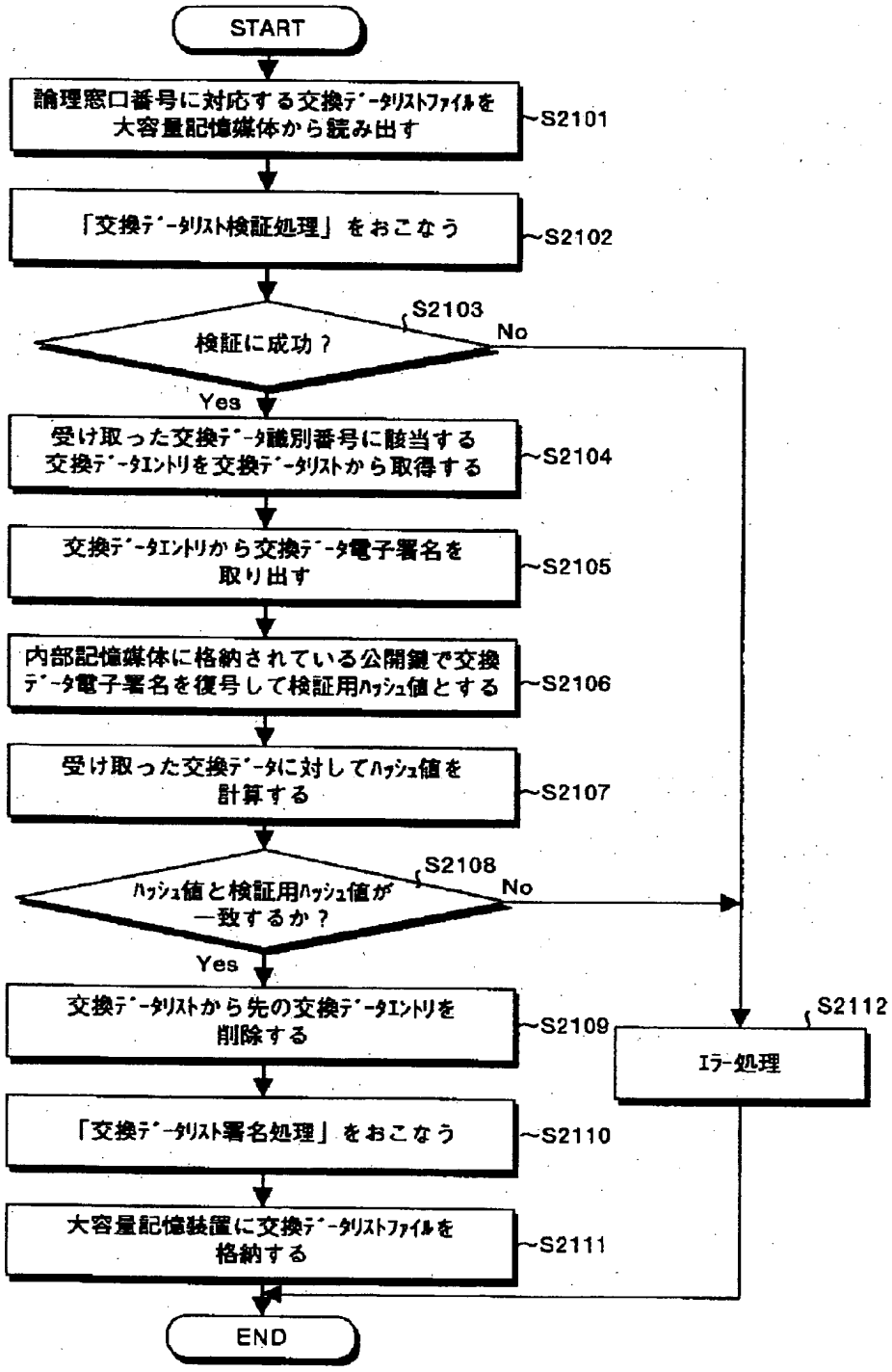
【図１９】


START
ﾕｰｻﾞのｱｶｳﾝﾄ名、受け取った論理窓口番号、ｱｸｾｽ種別（一覧）を元に「窓口ｱｸｾｽ権検査処理」をおこなう
S1901
ｱｸｾｽ権があるか？
S1902
No
Yes
大容量記憶装置から、受け取った論理窓口番号に対応する交換ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙを読み出す
S1903
「交換ﾃﾞｰﾀﾘｽﾄ検証処理」をおこなう
S1904
検証に成功？
S1905
No
Yes
交換ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙから交換ﾃﾞｰﾀ識別番号をすべて取り出し、交換ﾃﾞｰﾀ識別番号ﾘｽﾄを作成する
S1906
ｴﾗｰ処理
S1908
交換ﾃﾞｰﾀ識別番号ﾘｽﾄをﾕｰｻﾞ側に返す
S1907
END

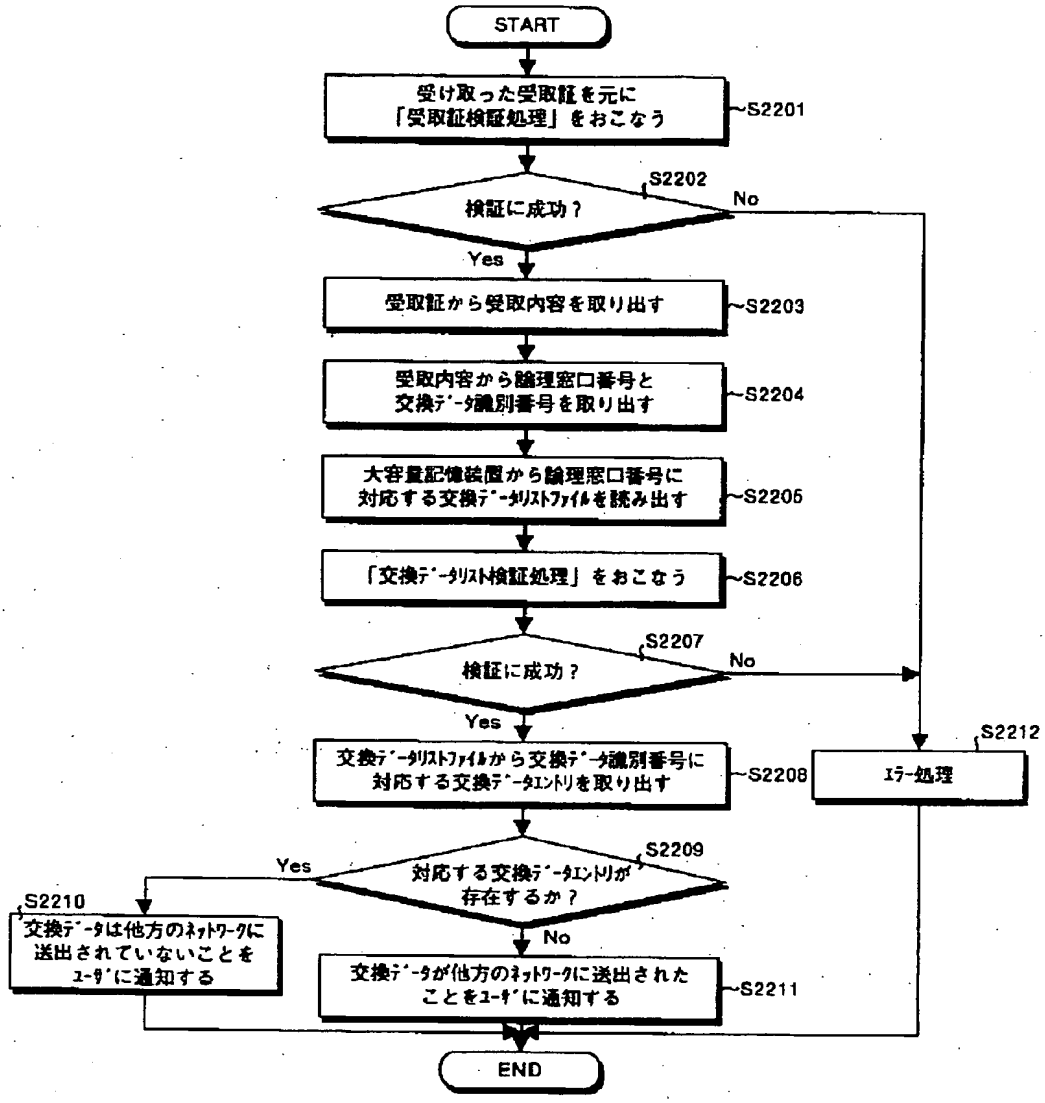
【図２０】


START
ﾕｰｻﾞのｱｶｳﾝﾄ名、受け取った論理窓口番号、ｱｸｾｽ種別（ﾘﾄﾘｰﾌﾞ）を元に「窓口ｱｸｾｽ権検査処理」をおこなう
S2001
ｱｸｾｽ権があるか？
S2002
No
Yes
論理窓口番号に対応するﾃﾞｨﾚｸﾄﾘから交換ﾃﾞｰﾀ識別番号に対応する交換ﾃﾞｰﾀを読み出す
S2003
交換ﾃﾞｰﾀ識別番号、交換ﾃﾞｰﾀを元に「交換ﾃﾞｰﾀﾘｽﾄ削除処理」をおこなう
S2004
処理が成功？
S2005
No
Yes
交換ﾃﾞｰﾀのﾌｧｲﾙを大容量記憶装置の論理窓口番号に対応するﾃﾞｨﾚｸﾄﾘから削除する
S2006
Ｉﾗｰ処理
S2008
交換ﾃﾞｰﾀをﾕｰｻﾞに送信する
S2007
END

【図２１】


START
論理窓口番号に対応する交換ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙを大容量記憶媒体から読み出す
S2101
「交換ﾃﾞｰﾀﾘｽﾄ検証処理」をおこなう
S2102
検証に成功？
S2103
No
Yes
受け取った交換ﾃﾞｰﾀ識別番号に該当する交換ﾃﾞｰﾀｴﾝﾄﾘを交換ﾃﾞｰﾀﾘｽﾄから取得する
S2104
交換ﾃﾞｰﾀｴﾝﾄﾘから交換ﾃﾞｰﾀ電子署名を取り出す
S2105
内部記憶媒体に格納されている公開鍵で交換ﾃﾞｰﾀ電子署名を復号して検証用ﾊｯｼｭ値とする
S2106
受け取った交換ﾃﾞｰﾀに対してﾊｯｼｭ値を計算する
S2107
ﾊｯｼｭ値と検証用ﾊｯｼｭ値が一致するか？
S2108
No
Yes
交換ﾃﾞｰﾀﾘｽﾄから先の交換ﾃﾞｰﾀｴﾝﾄﾘを削除する
S2109
S2112
ｴﾗｰ処理
「交換ﾃﾞｰﾀﾘｽﾄ署名処理」をおこなう
S2110
大容量記憶装置に交換ﾃﾞｰﾀﾘｽﾄﾌｧｲﾙを格納する
S2111
END

【図２２】



フロントページの続き

(72)発明者　谷内田　益義
東京都大田区中馬込１丁目３番６号　株式会社リコー内

Ｆターム(参考)　5J104 AA09 AA16 AA44 EA17 LA03 LA06 NA02 NA12 NA27 NA42 PA07
5K030 GA15 HA06 HB00 LA00 LD19
9A001 CC03 CC07 CC08 JJ13 JJ25 LL03